



FinCEN ADVISORY

FIN-2019-A006

August 21, 2019

Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids

Transnational criminal organizations (TCOs), foreign fentanyl suppliers, and Internet purchasers located in the United States engage in the trafficking of fentanyl, fentanyl analogues, and other synthetic opioids and the subsequent laundering of the proceeds from such illegal sales.

Introduction

This Advisory should be shared with:

- Chief Executive Officers
- Chief Operations Officers
- Chief Risk Officers
- Legal Departments
- Chief Compliance/BSA Officers
- AML Officials
- Sanctions Compliance Officials
- Cybersecurity Units

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory¹ to alert financial institutions to illicit financial schemes and mechanisms related to the trafficking of fentanyl, fentanyl analogues, and other synthetic opioids,² and to assist them in detecting and reporting related activity.

The United States is in the midst of an unparalleled epidemic of addiction and death, fueled by the illicit trafficking, sale, distribution, and misuse of fentanyl and other synthetic opioids. The statistics are sobering; between 2013 and 2017, deaths in the United States from synthetic opioids, other than methadone, increased over 800 percent.³ Every day in the United States, more than

130 people die from an opioid-related overdose.⁴ These numbers alone cannot fully capture the

1. This advisory is also part of a larger, United States government Fentanyl advisory covering the movement, manufacturing, marketing, and monetary aspects of the trafficking of fentanyl and other synthetic opioids. A summary of the *21st Century Drug Trafficking: Advisories on Fentanyl and Other Synthetic Opioids*, which includes links to each advisory, can be found here: <https://www.whitehouse.gov/wp-content/uploads/2019/08/White-House-Fentanyl-Advisories-Summary.pdf>.
2. The chemical names of synthetic opioids often sold online include: Acetylfentanyl, Butyrfentanyl, Carfentanil, FUF Fentanyl HCL, Furanylfentanyl, Isobutyrfentanyl, Lofentanil, 4'-methyl Acetyl fentanylHCL, Valerylfentanyl, and the U series, including U-47700. According to the Drug Enforcement Administration (DEA), informal slang terms for these variants include: 30s, Blues, Dragon's Breath, Fent, Fentanyl, Fenty, M-30s, etc. Additional slang words for fentanyl and other synthetic opioids can be found in the: [DEA Intelligence Report on Drug Slang CodeWords](#).
3. Centers for Disease Control and Prevention (CDC), National Center for Health Statistics, [Multiple Cause of Death Files, 1999-2017 CDC WONDER Online Database](#), December 2018. Accessed December 2018.
4. CDC/National Center for Health Statistics, [National Vital Statistics System](#), Mortality. CDC WONDER, Atlanta, GA: U.S. Department of Health and Human Services, CDC; 2018. <https://wonder.cdc.gov>.

F I N C E N A D V I S O R Y

devastation wrought by this epidemic, the consequences of which are far reaching and everlasting, from grieving parents and orphaned children, to the enormous economic and public policy costs,⁵ and the destruction of current and future generations.

The epidemic is tearing away at the social and economic fabric of our communities, while TCOs, international drug traffickers, money launderers, and other criminal actors profit off the misery of victims. Criminal networks and others generate billions of dollars in illicit drug proceeds, and use the U.S. financial system and economy to advance their criminal enterprises and continue this epidemic to generate more criminal profits, resulting in more deaths and addictions. FinCEN and other U.S. government agencies are collaboratively working with foreign partners, including Mexico, to end the fentanyl epidemic. This advisory will assist financial institutions in detecting and reporting suspicious activity, making it harder and more costly for criminals to (i) commit these crimes; (ii) hide and use their illicit money; and (iii) continue fueling this epidemic. By using the information in this advisory and safeguarding our financial system, financial institutions will help save lives, protect innocent families, and ensure the safety and future of our communities. Indeed, this is the real value and utility behind information generated, maintained, and reported under the Bank Secrecy Act by financial institutions. This advisory highlights the primary typologies and red flags derived from sensitive financial reporting which are associated with (i) the sale of these drugs by Chinese, Mexican, or other foreign suppliers; (ii) methods used by Mexican and other TCOs to launder the proceeds of fentanyl trafficking; and (iii) financial methodologies associated with the sale and procurement of fentanyl over the Internet by purchasers located in the United States.⁶ Fentanyl is sold in the United States in many forms, all of which can be deadly. Fentanyl can be purchased alone; mixed with heroin, cocaine, or methamphetamine; or pressed into pill form and falsely sold as prescription opioids, many times being ingested by unsuspecting victims.

Typologies

Fentanyl trafficking in the United States generally follows one of two pathways: direct purchase of fentanyl from China by U.S. individuals for personal consumption or domestic distribution; or cross-border trafficking of fentanyl from Mexico by TCOs and smaller criminal networks. Within these two categories, the predominant funding mechanisms associated with fentanyl trafficking patterns include: (i) purchases from a foreign source of supply made using money services businesses (MSBs), bank transfers, or online payment processors; (ii) purchases from a foreign source of supply made using

5. National Institute on Drug Abuse, "[Opioid Overdose Crisis](#)," January 2019.

6. Note that under U.S. federal law, fentanyl is a Schedule II controlled substance, which is lawfully produced and distributed in the United States by manufacturers of prescription drugs approved by the Food and Drug Administration and is widely used in medicine. This advisory focuses on the illicit manufacturing, importation, and/or distribution of illegal fentanyl and other synthetic opioids. Furthermore, while this advisory focuses on typologies involving fentanyl produced abroad and trafficked into the United States or purchased online, FinCEN is aware of trafficking in, and overprescribing of, pharmaceutical fentanyl in the United States and monitors and reports on illicit transactions associated with this activity.

F I N C E N A D V I S O R Y

convertible virtual currency⁷ (CVC) (such as bitcoin, bitcoin cash, ethereum, or monero); (iii) purchases from a U.S. source of supply made using an MSB, online payment processor, CVC, or person-to-person sales⁸; and (iv) other, more general money laundering mechanisms associated with TCO procurement and distribution.

*Direct Purchase of Fentanyl from China by U.S.
Individuals for Personal Consumption or Domestic Distribution*

**Purchases from a Foreign Source of Supply Using MSBs
Such as Money Transmitters or Online Payment Systems**

Transactions related to the sale or purchase of fentanyl often involve money transfers to individuals in China and other foreign countries through MSBs, online payment processors, or bank transfers to individuals located in foreign countries. An analysis of sensitive financial data illustrates that when U.S. individuals purchase fentanyl directly from China and other foreign countries, they often structure the money transfers to evade Bank Secrecy Act (BSA) reporting and recordkeeping requirements.⁹ Individuals frequently transfer the funds using multiple MSB agent locations. Additionally, although payment recipients may seem to be unrelated to one another, in many cases, they often share the same phone numbers.

These transactions generally begin with individuals located in the United States contacting foreign websites selling fentanyl or other prescription or illicit drugs¹⁰ regulated under the [Controlled Substances Act](#). The websites, which are typically registered to or operated by individuals located in China, direct users to contact a representative of the company or individual by telephone, message (e.g., video messaging, text messages, or the use of messaging applications), or email.

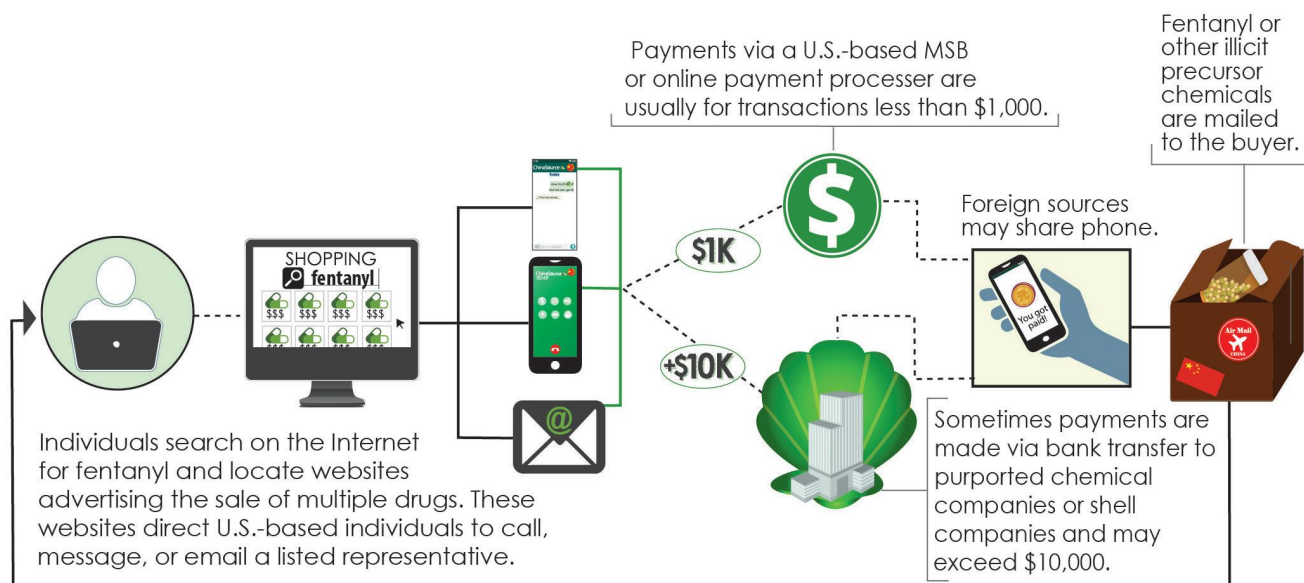
Once the buyer and the sales representative come to an agreement, the sales representative typically directs the buyer to send the payment to a particular person through an MSB located in the United States, online payment processor, or bank transfer (*see Figure 1*). The contact information often includes a telephone number, which may be associated with the foreign-based website and may also be used by many other foreign payment recipients or likely couriers. The payments to these foreign sources are typically low-dollar-value transactions (less than \$1,000), sometimes conducted through multiple transactions or in a single transaction. In other cases, the

-
7. A type of virtual currency that either has an equivalent value in real currency or acts as a substitute for real currency. [FIN-2013-G001](#), "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013; *see also* [FIN-2019-G001](#), "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," May 9, 2019, and [FIN-2019-A003](#), "Advisory on Illicit Activity Involving Convertible Virtual Currency," May 9, 2019.
 8. Person-to-person in this context, refers to the physical method of meeting in person and exchanging cash for fentanyl.
 9. "Structuring," as the term is used in statute for criminal activity (*see* 31 U.S.C. §5324), includes not only attempts to evade reporting requirements, but also attempts to evade the Travel Rule and related recordkeeping requirements. FinCEN's regulations on structuring (*see generally* 31 CFR § 1010.100(xx) and 31 CFR § 1010.314) focus on evasion of cash transaction reporting (CTR) requirements.
 10. To include fentanyl analogues or other synthetics with no legitimate medical use.

F I N C E N A D V I S O R Y

foreign supplier may direct the individual to send a bank transfer directly to a front company operating in the chemical manufacturing field or to a shell company that is unrelated to chemicals or chemical production activity. These payments are typically higher-dollar-value transactions (over \$10,000) and may be associated with bulk drug or precursor chemical purchases.¹¹ These companies, or their representatives, then typically mail or ship the illicit narcotics directly to the buyers in the United States for personal consumption or redistribution.¹²

Figure 1: MSB, Online Payment Processor, or Bank Transfer to Foreign-based Contact



Purchases from a Foreign-located Supplier Using CVC

Drug traffickers and consumers increasingly use Clearnet and Darknet¹³ e-commerce markets, paired with online payment systems and virtual currencies, to further anonymize fentanyl purchase and distribution.¹⁴ An analysis of sensitive financial data indicates that domestic illicit drug manufacturers, dealers, and consumers use online payment platforms or CVC to purchase precursor chemicals or completely synthesized narcotics primarily sourced from China.

11. Fentanyl precursor chemicals refer to the basic or parent chemicals that form fentanyl. See [Controlled Substances Act](#) and the [List of Controlled Substances](#).

12. See DEA, [2018 National Drug Threat Assessment](#), October 2018.

13. The Internet is typically separated into three distinct parts: (i) the open Internet, also known as the Clearnet, which encompasses sites publicly accessible through well-known and publicly advertised search engines; (ii) the Deep Web, which consists of content not indexed and sites that cannot be found by normal search functions, such as paywall-protected pages; and (iii) the Darknet, which consists of many segments, which are areas of the Internet accessible only via specialized anonymizing software, such as the The Onion Router (Tor) network. (Sites only reachable through the Tor network are recognizable through their “.onion” URL domain suffix.) While Darknet content is varied, it is also home to hidden services such as criminal marketplaces that allow individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet. Generally, these Darknet market websites use a variety of anonymizing and encryption technologies in an attempt to shield communications and transactions from interception and monitoring.

14. See DEA, [2018 National Drug Threat Assessment](#), October 2018.

FINCEN ADVISORY

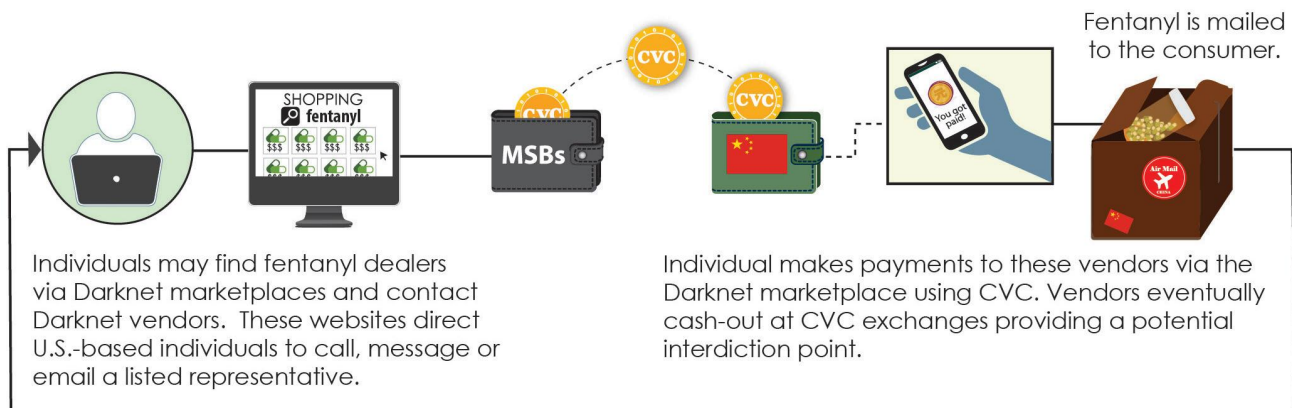
Filing institutions have identified potential drug traffickers based on embedded messages or references on websites that mention illegal drug transactions using CVC exchangers.¹⁵ Such messages and websites provide valuable financial intelligence on the source or destination of money and products.

CVC Payment to Foreign Contact Method

Similar to purchases from a foreign source of supply using MSBs or online payment processors, individuals located in the United States search for fentanyl and identify potential websites that may provide the opportunity to purchase illicit drugs online. Foreign representatives will instruct the U.S.-based individual to send payments through CVC, such as bitcoin, bitcoin cash, ethereum, or monero¹⁶ (see Figure 2).

Additionally, U.S.-based individuals may find fentanyl dealers on Darknet markets and contact Darknet vendors located worldwide, including in the United States. Individuals purchasing fentanyl on the Darknet will also pay vendors using CVC. Darknet vendors and chemical companies then mail the illicit narcotics directly to the U.S.-based individuals. The Darknet vendors may eventually seek to exchange CVC for traditional fiat currency such as U.S. dollars (USD) using both U.S.- and foreign-based CVC exchangers, or sell the virtual currency themselves to the public as unlicensed money transmitters.¹⁷ Higher-amount transactions, coupled with other suspicious indicators, are more likely to be related to a vendor, redistributor, or street dealer compared with the activity of a personal consumer.

Figure 2: CVC Payment to Foreign-based Contact Method



15. An “exchanger” is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. See [FIN-2019-G001](#), “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies,” May 9, 2019; and see also [FIN-2013-G001](#), “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,” March 18, 2013.

16. FinCEN notes these are just examples of CVCs and that other types of CVCs may be also be used.

17. FinCEN regulations define “money transmitter” to include a “person that provides money transmission services” or “any other person engaged in the transfer of funds.” 31 CFR § 1010.100(ff)(5).

F I N C E N A D V I S O R Y

*Purchases from a U.S.-located Supplier Using an MSB,
Online Payment Processor, CVC, or Person-to-Person Transaction*

Individuals located in the United States use the Internet or local connections to buy fentanyl from suppliers who are also located in the United States. In this type of transaction, individuals typically make payments in one of two ways. First, payments can be made using both MSBs and online payment platforms, similar to the way payments are made to foreign suppliers. After the payment is received, the supplier typically ships or mails the fentanyl to the consumer.¹⁸ Second, in more traditional drug trafficking transactions, individuals make payments in person with cash (person-to-person transactions). In this scenario, fentanyl is hand-delivered in exchange for cash, and then the drug traffickers deposit or launder the cash. The cash transaction dollar values may vary depending on variables, such as geographic location and the amount (or weight) of the illicit narcotics that are purchased.

*Cross-border Trafficking of Fentanyl
by TCOs and Smaller Criminal Networks*

TCO Procurement and Distribution

Mexico is a transit and production point for the trafficking of many illicit drugs and Mexican TCOs operate as the dominant purveyors of these illicit drugs, which also include fentanyl.¹⁹ Mexican TCOs control the smuggling routes across the Southwest Border (SWB) and arrange the transport and distribution of fentanyl throughout the United States.²⁰

Subsequently, Mexican TCOs arrange the consolidation, placement, and movement of illicit proceeds derived from fentanyl sales in the United States. FinCEN's review of confidential financial information reveals transactions that involve structured cash deposits, money transfers, and wire transfers for the ultimate credit of accounts in the U.S. SWB region and Mexico. FinCEN finds that this confidential financial information frequently describes individuals who conduct excessive cash transactions using ATMs, unsourced cash, and no verifiable or legitimate purpose for the transactions. Drug trafficking networks often use shell companies to disguise the illicit drug proceeds as legitimate business transactions. BSA data also shows that individuals located in the United States use their accounts to funnel funds between domestic and international locations. Some of the more common money laundering methodologies used by Mexican TCOs are described below:

18. One common thread among these transactions is the potential use of mailing and shipping systems to disseminate fentanyl. Traffickers regularly ship fentanyl and its analogues through the mail to drug dealers and users in the United States. The shippers often layer transactions and mask their identities, making it difficult for the Postal Inspection Service or Customs and Border Protection to identify which packages, among the hundreds of thousands arriving every day, contain illicit drugs.

19. See DEA, [2018 National Drug Threat Assessment](#), p. 21, October 2018.

20. See DEA, [2018 National Drug Threat Assessment](#), pp. 33-34, October 2018.

FINCEN ADVISORY

1. *Bulk Cash Smuggling*²¹: To smuggle bulk cash across the border from the United States to Mexico, a TCO, or a third party it retains, conceals more than \$10,000 in currency or other monetary instruments on a person, luggage, or in any conveyance for transportation from a place within the United States to a place in Mexico.

U.S. law enforcement suspects that most bulk currency smuggled into California from other U.S. states is payment for drug shipments.²² The majority of this illicit bulk currency is then transported across the border into Mexico through privately owned vehicles or commercial tractor-trailers.²³

2. *Trade-Based Money Laundering*: Large amounts of bulk cash resulting from illegal drug sales, including fentanyl, can be difficult to transport across U.S. borders undetected, prompting drug traffickers to look to less conspicuous alternatives, such as trade-based money laundering (TBML) schemes. TBML often involves using illicit proceeds to buy goods for export, as the subsequent sale of the goods effectively launders the proceeds.²⁴ The Financial Action Task Force (FATF) defines TBML as, “the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. Moreover, TBML techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail.”²⁵ In this context, TBML often involves converting physical U.S. banknotes into a commodity and then exporting or importing the commodity, without physical cross-border movement of the underlying currency.²⁶ For example, drug traffickers will convert the monetary value of bulk currency (i.e., banknotes) into a good with an equivalent monetary value, such as a smartphone, automobile, or jewelry.

To facilitate TBML, a TCO transfers funds from the United States back to international jurisdictions using either internal accountants or an independent accountant, also referred to as a “money broker.” The following TBML example uses an external broker in Mexico (*see Figure*

21. In 2017, California, Ohio, and Arizona reported the highest dollar amounts in bulk cash seizures for a combined total of \$138.8 million. This amount decreased significantly, by approximately 49 percent, in comparison to the previous year’s top-three grossing states for seizures. *See* Deputy Chief of Operations Office of Global Enforcement, DEA, “[Statement Before The Subcommittee on Border Security and Immigration](#),” United States Senate, December 12, 2018.

22. Deputy Chief of Operations Office of Global Enforcement, DEA, “[Statement Before The Subcommittee on Border Security and Immigration](#),” United States Senate, December 12, 2018.

23. *Ibid.*

24. *See* [2018 National Money Laundering Risk Assessment \(2018 NMLRA\)](#).

25. *See* FATF, [Trade Based Money Laundering](#), p. i, June 23, 2006.

26. *See* FinCEN Advisory, “Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML,” [FIN-2014-A005](#), May 28, 2014; and *see* [2018 NMLRA](#).

F I N C E N A D V I S O R Y

3).²⁷ The TCO and broker negotiate a money pick-up and transfer a commission fee prior to the TBML operation. The TCO then informs the broker where to pick up the USD drug proceeds using an encrypted code, as a proceeds confirmation or validation means. The broker may use an assistant or hire launderers (often called “smurfs”) to pick up the proceeds on the broker’s behalf. Upon proceeds pick-up, the launderers may:

- i. deposit proceeds into U.S. financial institutions (often structured to avoid recordkeeping and reporting requirements) and then transfer the funds as goods or debt payments to U.S. vendors and exporters; or
- ii. transport (also called “drop” or “hand off”) the bulk cash to third parties, including U.S. exporters, for subsequent deposit and integration into the U.S. financial system.

Prior to the money pick-up, the money broker negotiates a contract and exchange rate with a Mexican importer to pay for exported USD-denominated goods on the importer’s behalf (i.e., a third-party payment). Once the broker receives the Mexican peso-denominated deposits from the importer, the broker’s account is “loaded,” and he can then facilitate the money pick-up by the launderer(s) or smurf(s) and make a simultaneous payment to the TCO to reconcile accounts. In this type of offsetting transaction, often called a “mirror transfer,”²⁸ the launderer picks up the money, and confirms that the broker received the proper amount (normally via text or a phone call), and the broker then transfers or “hands off” a peso-equivalent amount of USD to the TCO. Sometimes this type of transaction commences when the Mexican importer pays the broker (thereby “loading” his account) prior to the initial money drop in the United States.

The vendor who receives USD from the launderer will then export the goods to the Mexican importer according to the money broker’s shipping directions. After receiving the goods, the importer sells them on the Mexican open market at a markup, and the importer’s account is reconciled or balanced.

27. There are many Black Market Peso Exchange variations, including nuances to this scenario. TBML elements and the types of players in these transactions are normally consistent. Also, while this advisory is specific to fentanyl trafficking from Mexico, the TBML methodology can also be used with many countries, to include Central/South America.

28. See DEA, [2017 National Drug Threat Assessment](#), p. 128, October 2017.

F I N C E N A D V I S O R Y

Figure 3: Trade-based Money Laundering



3. Structured MSB Money Transfers: Professional money laundering organizations hire loosely associated parties (including “money mules”²⁹) to send money transfers to Mexico via U.S. MSBs, primarily money transmitters, structured to evade reporting requirements. In this context, structuring (i.e., keeping the amount of the money transfer below the applicable threshold of \$3,000 in order to avoid identification and reporting requirements) is accomplished through one of, or a combination of, the following:
- The illicit proceeds are divided between multiple individuals who send the transfers;
 - An individual uses multiple MSB agent locations to send transfers; and/or
 - An individual sends multiple transactions consecutively.

29. The Federal Bureau of Investigation (FBI) defines “money mule” as “someone who transfers illegally acquired money on behalf of or at the direction of another.” FBI, [Money Mule Awareness Booklet](#), p. 2, December, 2018.

FINCEN ADVISORY

4. *Funnel Account Activity*: Multiple individuals acting on behalf of the TCO deposit cash proceeds of illicit drug sales into a personal or business account. The deposits are often made in multiple states geographically distant from the branch in which the account was opened or domiciled and geographically different from the location of the withdrawal activity.³⁰ The deposits are structured (i.e., kept below the applicable threshold of \$10,000, in this instance, to avoid identification and recordkeeping requirements).³¹ The use of funnel account activity by TCOs may have been partially disrupted by the decisions of certain large national banks to restrict third-party cash deposits for private customer accounts.

Case Studies of Fentanyl-related Illicit Finance

Example of Funnel Accounts Funding Wires to Mexico Disguised as Legitimate Business

Financial Institution Type: *Depository Institutions*

In December 2018, a federal jury convicted Herman E. Aguirre and Troy R. Gillon of narcotics conspiracy. Aguirre was also convicted of operating a continuing criminal enterprise and money laundering conspiracy.³² In 2016, these two individuals were indicted along with 15 co-conspirators for their role in a criminal network of individuals and food and produce companies affiliated with the Sinaloa Cartel trafficking in thousands of kilograms of heroin, fentanyl, and cocaine from Mexico into the United States by disguising the shipments in pallets described as containing “sea cucumbers.”³³ The TCO’s operation spanned Mexico, Arizona, California, and elsewhere, with the Sinaloa Cartel, led by Joaquín “El Chapo” Guzmán and Ismael “El Mayo” Zambada, as its source of supply.³⁴ The TCO opened accounts in banks in southern California, which were used to receive cash deposits at drug sale locations in Northeastern cities.³⁵

30. See FinCEN Advisory, “Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML”, [FIN-2014-A005](#), (May 2014).

31. *Ibid.*

32. Department of Justice, U.S. Attorney’s Office, Western District of New York, “[Federal Jury Convicts Two Defendants of Narcotics Conspiracy Tied To The El Chapo Mexican Drug Cartel](#),” December 20, 2018.

33. Western District of New York, “[17 Defendants Indicted in International Drug Trafficking Ring](#),” August 9, 2016.

34. Department of Justice, U.S. Attorney’s Office, Western District of New York, “[Federal Jury Convicts Two Defendants of Narcotics Conspiracy Tied To The El Chapo Mexican Drug Cartel](#),” December 20, 2018.

35. Western District of New York, “[17 Defendants Indicted in International Drug Trafficking Ring](#),” August 9, 2016.

F I N C E N A D V I S O R Y

Darknet and Clearnet Marketplace Fentanyl Transactions**Financial Institution Type:** MSBs and Depository Institutions

Matthew and Holly Roberts were sentenced to 135 and 96 months in federal prison, respectively, for their roles in distributing fentanyl and other narcotics through multiple Darknet marketplace³⁶ accounts.³⁷ At the time of their arrest in 2018, the couple were the most prolific Darknet fentanyl vendors in the world. They used “private messaging, encryption software, Virtual Private Networks and proxies through the Tor network” as well as pre-paid Visa and gift cards, and mailed decoy items, such as glow bracelets, to hide the fact they were mailing narcotics.³⁸

Their customers made purchases with virtual currency, which the couple then sent to virtual currency exchangers to convert the funds into U.S. fiat currency.³⁹

Note: Based on analysis of sensitive financial data, Holly Roberts added funds to stored value cards and immediately removed funds via ATM withdrawals and online purchases. Matthew Roberts and associates received excessive cash deposits into their accounts from sources outside of the account’s geographic area followed immediately by cash withdrawals.

Kingpin Act Sanctions – Chinese Synthetic Opioid Traffickers

Through sanctions investigations into Chinese nationals involved in synthetic opioid trafficking, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) designated Chinese national Jian Zhang as a significant foreign narcotics trafficker, the first fentanyl-related designation pursuant to the Foreign Narcotics Kingpin Designation Act (Kingpin Act).⁴⁰ Zhang’s trafficking of fentanyl and other controlled substances to the United States was tied to the overdose deaths of U.S. citizens. In addition to Zhang, OFAC designated a chemical company named Zaron Bio-Tech (Asia) Limited, a Hong Kong entity operating in Shanghai, China, that was owned and controlled by Zhang. Zhang used Zaron Bio-Tech to facilitate

36. Dream Market, Silk Road, AlphaBay, Darknet Heroes League, Nucleus, and several others.

37. Department of Justice, U.S. Attorney’s Office, Northern District of Ohio, [“Texas couple sentenced to prison; they were the most prolific dark net fentanyl vendor in the world at the time of their arrest last year,”](#) February 7, 2019. Department of Justice, U.S. Attorney’s Office, Northern District of Ohio, [“Texas couple who had thousands of online sales of fentanyl and other drugs pleaded guilty to drug crimes,”](#) October 23, 2018. Department of Justice, Office of Public Affairs, [“Operation Darkness Falls Results in Arrest of One of the Most Prolific Dark Net Fentanyl Vendors in the World,”](#) August 22, 2018.

38. Department of Justice, U.S. Attorney’s Office, Northern District of Ohio, [“Texas couple sentenced to prison; they were the most prolific dark net fentanyl vendor in the world at the time of their arrest last year,”](#) February 7, 2019.

39. Department of Justice, Office of Public Affairs, [“Operation Darkness Falls Results in Arrest of One of the Most Prolific Dark Net Fentanyl Vendors in the World,”](#) August 22, 2018.

40. See Treasury Press Release: [“Treasury Sanctions Chinese Fentanyl Trafficker Jian Zhang,”](#) April 27, 2018.

F I N C E N A D V I S O R Y

the unlawful importation of fentanyl and other controlled substances into the United States. OFAC also designated four individuals, including Zhang's mother and father, who assisted his narcotics trafficking activities by using global MSBs to receive funds for fentanyl purchases from individuals located in the United States.⁴¹

In 2014, OFAC sanctioned two Chinese nationals, Bo Peng and Zhang Lei, as specially designated narcotics traffickers pursuant to the Kingpin Act,⁴² as well as two Chinese companies, CEC Limited and Kaikai Technology Co., Ltd., for their role in international drug trafficking relating to synthetic opioids, cannabinoids, and cathinones. OFAC also designated three additional Chinese nationals for their role on behalf of Zhang Lei.⁴³

Darknet Fentanyl Purchases

The Darknet is commonly used for a number of illicit activities, including fentanyl trafficking. In July 2017, the U.S. Department of Justice seized AlphaBay servers and assets; AlphaBay was the largest criminal Darknet market on the Internet at the time.⁴⁴ AlphaBay required its users to transact in CVC (including bitcoin, monero, and ethereum) to obfuscate transactions and related parties. The Darknet site was a major platform for transactions involving fentanyl and heroin, which were linked to overdose deaths. AlphaBay operated for over two years on the Darknet, and hundreds of thousands of people around the world used the site to buy and sell deadly and illegal drugs, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals. U.S. officials estimate, based on the law enforcement investigation, that AlphaBay was used to launder hundreds of millions of dollars linked to its illegal transactions.⁴⁵

Red Flag Indicators for Fentanyl-related Activity

The red flags noted below may help financial institutions in identifying suspected schemes related to illicit fentanyl trafficking. Some red flags listed may also be applicable more generally to drug trafficking, or apply to other trafficked drugs, or to other money laundering or illicit activity, but are detailed in order to provide context for financial activity related to fentanyl. In applying the red flags, financial institutions are advised that no single transactional red flag necessarily indicates suspicious activity conclusively. Financial institutions may consider additional contextual information and the surrounding facts and circumstances, such as a customer's historical

41. *Ibid.*

42. See Treasury Press Release: "[Treasury Sanctions Prolific Chinese Synthetic Drug Traffickers](#)," April 27, 2018.

43. See Treasury Press Release: "[Treasury Sanctions Members of a Chinese Synthetic Drug Trafficking Organization](#)," July 29, 2014.







44. U.S. Department of Justice, "[AlphaBay, Largest Online Dark Market, Shut Down](#)," July 20, 2017.

45. *Ibid.*




F I N C E N A D V I S O R Y

financial activity and whether the customer exhibits multiple indicators, before determining that a transaction is suspicious. Financial institutions may also perform additional inquiries and investigations where appropriate.


MSBs: Money Transfer Red Flags

-  1 The money transfer beneficiary lists a phone number or email address associated with a pharmaceutical company or chemical sales website.
-  2 U.S. remitter sends low-dollar money transfers to an individual in China for no apparent legitimate purpose. Individual transfers may range from \$10 to \$100, with an aggregated amount of multiple transfers totaling approximately \$600. Conversely, a U.S. remitter sends a high volume of money transfers to apparently unrelated individuals.
-  3 Multiple U.S. remitters send money transfers to the same individual beneficiary in China (i.e., many to one).
-  4 Seemingly unrelated beneficiaries share the same phone number or email address to receive transactions.
-  5 The volume of outgoing money transfers is not consistent with the expected activity of a U.S. remitter.
-  6 A U.S. remitter adjusts the money transfer amount to avoid BSA reporting and recordkeeping requirements (i.e., structuring). When a U.S. remitter sends multiple structured money transfers, additional red flags may be involved:
 - Remitter uses multiple agent locations.
 - Remitter sends money transfers to the same beneficiary consecutively, instead of aggregated in a single sum.
 - Two or more seemingly unrelated remitters are linked together by shared attributes such as common addresses or profile information. These remitters then coordinate transactions to evade the recordkeeping threshold.


Depository Institutions: Structuring and Funnel Account Activity Red Flags

-  7 Account owners or third parties structure cash deposits at bank branches nationwide into the same account, which funds outgoing transactions on the SWB, including cash withdrawals or wire transfers to Mexico (i.e., funnel account activity and rapid movement of funds).
-  8 The depository institutions have a suspicion concerning the physical condition of deposited banknotes (e.g., the bills smell of drugs, detergent, or are excessively worn).
-  9 The source of funds cannot be corroborated.

F I N C E N A D V I S O R Y

 10 Multiple transactions below the applicable Currency Transaction Report (CTR) threshold (i.e., structuring), which may involve additional indicators:

- Suspicious use of multiple locations.
- Two or more individuals working together.
- Suspicious use of multiple accounts.

 11 Transaction out of pattern for customers or business type.

 12 Transaction with no apparent business purpose.

Depository Institutions: Shell Company Red Flags

 13 Unclear business model:

- The company's North American Industry Classification System (NAICS) code(s) is/are in a different industry than the business name indicates.
- Commercial databases reveal the company is associated with multiple businesses in unrelated industries.
- Open source information reveals that the company lacks or has vague company websites.

 14 Company address or location discrepancy:

- Online or other open source searches on the address provided reveal a business with a different name, or an operating location inconsistent with the business model, such as a residence.
- Commercial databases associate the company with multiple active addresses or operating locations, but reveal few, if any, indications the company has franchises or multiple branches, subsidiaries, or agents.

 15 Company name discrepancy:

- The company's name is vague, non-descriptive, or does not align with its business model.
- Commercial databases reveal the company has three or more name variations or has multiple "doing business as" (dba) names.

 16 Employer Identification Number (EIN) discrepancy:

- Commercial databases reveal the company is a small business with fewer than 500 employees but has multiple EINs or shares EINs with other businesses.


F I N C E N A D V I S O R Y

*Depository Institutions and MSBs:
Clearnet and Darknet Marketplace Fentanyl Purchase Red Flags*

 Direct or indirect transactions with Darknet marketplaces or CVC mixing services.⁴⁶ The names of several current popular Darknet marketplaces include:⁴⁷

- Empire
- Tochka/Point
- Valhalla
- Rapture
- Berlusconi

 Customers with past criminal histories for drug-related offenses.

 Customers discussing drug purchases in the transaction notes field available on the exchange, including referencing drugs or weight measurements like grams (e.g., “1 gram fent”). Customers may reference the informal slang names⁴⁸ (e.g., “Fenty”) or the actual chemical names (e.g., “Acetylfentanyl”).

 Use of virtual private network (VPN) services or Tor to access CVC exchange accounts.

Valuable Information in Reporting Suspicious Activity

Suspicious Activity Involving Websites and Embedded Messages

Online payment systems or CVC exchangers may have access to embedded messages or other information that reference Internet purchases of illegal drugs. This information can be extremely useful for financial institutions in determining suspicious activity linked to potential drug trafficking and to law enforcement for investigative purposes.

Suspicious Activity Involving CVC

CVC transactions generate a significant variety of information elements that may be extremely useful to law enforcement in investigating potential illicit conduct involving CVC transactions. Specifically, the following information is particularly helpful to law enforcement:

- virtual currency wallet addresses

46. Tumbling or mixing involves the use of mechanisms to break the connection between an address sending CVC and the addresses receiving CVC.

47. See the Red Flag section of the “Marketing Advisory,” which is a part of a larger, United States government Fentanyl advisory covering the movement, manufacturing, marketing, and monetary aspects of the trafficking of fentanyl and other synthetic opioids. A summary of the *21st Century Drug Trafficking: Advisories on Fentanyl and Other Synthetic Opioids*, which includes links to each advisory, can be found here: <https://www.whitehouse.gov/wp-content/uploads/2019/08/White-House-Fentanyl-Advisories-Summary.pdf>.

48. See DEA Intelligence Report on [Drug Slang Code Words](#).

F I N C E N A D V I S O R Y

- account information
- transaction details (including virtual currency transaction hash)
- relevant transaction history
- available login information (including IP addresses)
- mobile device information (such as device International Mobile Equipment Identity (IMEI))
- information obtained from analysis of the customer's public, online profile and communications (such as device International Mobile Equipment Identity (IMEI))

When filing a Suspicious Activity Report (SAR), financial institutions should provide all pertinent available information in the SAR form and narrative.

Reminder of Regulatory Obligations for U.S. Financial Institutions

Consistent with existing regulatory obligations, U.S. financial institutions should take reasonable, risk-based steps to identify and limit any exposure they may have to funds and other assets associated with individuals and entities engaged in the financial facilitation or trafficking in fentanyl or other synthetic opioids.

Reminder of Anti-Money Laundering (AML) and Regulatory Obligations for U.S. Financial Institutions Regarding Due Diligence, Customer Identification, and Suspicious Activity Reporting

FinCEN is providing the information in this advisory to assist U.S. financial institutions in meeting their risk-based due diligence and other BSA obligations to help identify individuals who may be engaged in the financial facilitation or trafficking in fentanyl or other synthetic opioids.

Enhanced Due Diligence Obligations

FinCEN reminds U.S. financial institutions that they must comply with their due diligence obligations under the BSA and its implementing regulations.⁴⁹ In addition to their general due diligence requirements, covered financial institutions are required to implement a due diligence program for private banking accounts held for non-U.S. persons designed to detect and report any known or suspected money laundering or other suspicious activity through those accounts.⁵⁰

49. See 31 U.S.C § 5318(h) and 31 CFR § 1010.210 for AML program requirements, and as applied to specific financial institutions in 31 CFR §§ 1020.210, 1021.210, 1022.210, 1023.210, 1024.210, 1025.210, 1026.210, 1027.210, 1028.210, 1029.210, and 1030.210.

50. See USA PATRIOT Act § 312, codified at 31 U.S.C. § 5318(i) and 31 CFR § 1010.620(a). The definition of "covered financial institution" is found in 31 CFR § 1010.605(e). The definition of "private banking account" is found in 31 CFR § 1010.605(m). The definition for the term "non-U.S. person" is found in 31 CFR § 1010.605(h).

F I N C E N A D V I S O R Y

FinCEN also reminds covered financial institutions of their obligation to implement due diligence programs for correspondent accounts they maintain for foreign financial institutions that include appropriate, specific, risk-based and, where necessary, enhanced policies, procedures, and controls reasonably designed to detect and report known or suspected money laundering activity involving such accounts.⁵¹

Customer Identification

In addition, certain financial institutions also must have a written customer identification program,⁵² to allow the institution to form a reasonable belief that it knows the true identity of each of its customers. At a minimum, these financial institutions must, at account opening, obtain and verify each customer's name, date of birth for individuals listed on the account, address, and identification number.⁵³

An MSB's AML program must establish adequate and appropriate procedures and controls commensurate with the money laundering and terrorist financing risks posed by foreign agents or counterparties with which that MSB does business.⁵⁴

Suspicious Activity Reporting

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.⁵⁵

SAR Filing Instructions

When filing a SAR, financial institutions should provide all pertinent available information in the SAR form and narrative. **FinCEN requests that financial institutions use only the updated mandatory SAR form (as of February 1, 2019) and reference this advisory using the following key term in SAR field 2 (Filing Institution Note to FinCEN):**

"FENTANYL FIN-2019-A006"

to indicate a possible connection between the suspicious activities being reported and activities highlighted in this advisory.

51. See USA PATRIOT Act § 312 (31 U.S.C. § 5318(i)); 31 CFR § 1010.610(a).

52. See 31 CFR §§ 1020.220, 1023.220, 1024.220, and 1026.220.

53. See, e.g., 31 CFR § 1020.220.

54. See FinCEN [Interpretive Release 2004-1](#), 69 FR 239, December 14, 2004.

55. See 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.

F I N C E N A D V I S O R Y

SAR reporting, in conjunction with effective implementation of due diligence requirements and OFAC obligations by financial institutions, has been crucial to identifying proliferation financing as well as money laundering and terrorist financing. SAR reporting is consistently beneficial and critical to FinCEN and U.S. law enforcement analytical and investigative efforts, OFAC designation efforts, and the overall security and stability of the U.S. financial system.⁵⁶

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at frc@fincen.gov.

Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day). The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

56. For Law Enforcement Case Examples, see [SAR Activity Review, Issue 19](#), beginning on p. 19.

UNITED STATES DISTRICT COURT

for the

Eastern District of California

FILED**Mar 14, 2022**CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA**SEALED**

United States of America

v.

Case No.

2:22-mj-0045 DB

Jose Manuel CHAVEZ Zepeda and Denis Zacarias
PONCE Castillo*Defendant(s)***CRIMINAL COMPLAINT**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of April 22, 2016 through the present in the county of Sacramento in the
date
Eastern District of California, the defendant(s) violated:*Code Section**Offense Description*

COUNT ONE – 21 U.S.C. §§ 841(a)(1) and 846 - Conspiracy to Distribute and Possess with Intent to Distribute at least 500 grams of a Mixture and Substance containing Cocaine (April 22, 2016 through the present)

COUNT TWO – 21 U.S.C. § 841(a)(1) - Distribution of at least 500 grams of a Mixture and Substance containing Cocaine (June 25, 2021)

This criminal complaint is based on these facts:

(see attachment)

☒ Continued on the attached sheet.

/s/ Orcina Pacheco-Garcia

Complainant's signature

FBI Special Agent Orcina Pacheco-Garcia

Printed name and title

Sworn to me and signed telephonically.

Date: 03/14/2022City and state: Sacramento, California

DEBORAH BARNES

UNITED STATES MAGISTRATE JUDGE

000323

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT AND CRIMINAL COMPLAINT

I, Orcina Pacheco Garcia, Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

Background and Expertise

1. I am a Special Agent with the FBI. I entered on duty at the FBI Academy in Quantico, Virginia, in March 2019. I am currently assigned to the Sacramento Strike Force. I have been assigned to this squad since 2022.
2. During the course of my employment as an FBI Special Agent, I have participated in numerous criminal investigations. I have worked for the FBI in other capacities since September 2017. Based on my training and experience as an agent with the FBI, I have investigated federal criminal violations related to, among other things, narcotics trafficking, child exploitation and child pornography, kidnappings, and human trafficking. I have participated in numerous investigations involving the use of federal and state search warrants to collect evidence, including controlled substances, the seizure of narcotics-related records, and other types of evidence that document the activities of criminal organizations in both the manufacturing and distribution of controlled substances and weapons.
3. I am an “investigative or law enforcement officer” of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am an officer of the United States empowered by law to conduct criminal investigations and make arrests for offenses enumerated in 18 U.S.C. § 2516.
4. Because this affidavit is submitted for the limited purpose of establishing probable cause for the requested complaint, search and arrest warrants, I have not included each and

every fact known to me about this case. Rather, I have set forth only the facts that I believe are necessary to support probable cause.

5. This affidavit is based upon my own personal knowledge and upon the knowledge of other law enforcement officers involved in this investigation. Where I describe statements made by other people (including other special agents and law enforcement officers), the statements are described in sum, substance, and relevant part. Similarly, where I describe information contained in reports and other documents or records in this affidavit, this information is described in sum, substance, and relevant part.

Scope of Requested Search Warrants

6. This affidavit is submitted in support of an application for warrants to search the locations and vehicles further described below and in **Attachments A-1 through A-17**. The contraband, objects, and information for which we will search are described in **Attachment B**. Attachments A-1 through A-17 and Attachment B are incorporated by reference.

7. This Affidavit is submitted in support of warrants to search the following locations, telephones, and vehicles:

- a. The residence located at **3505 Condor Court, Carmichael, California** (“**Target Location 1**”), residence of Jose CHAVEZ as described in Attachment A-1;
- b. The business located at **2533 Del Paso Boulevard, Sacramento, California, known as La Victoria Supermercado**, (“**Target Location 2**”), business of Jose CHAVEZ described in Attachment A-2;
- c. The residence located at **2556 Rio Linda Boulevard, Sacramento, California** (“**Target Location 3**”), suspected drug stash house controlled by Jose CHAVEZ, described in Attachment A-3;

- d. The residence located at **2480 Larkspur Lane, #176, Sacramento, California** (“**Target Location 4**”), residence of Denis PONCE described in Attachment A-4;
- e. The residence located at **1412 Thomasnell Way, Ceres, California** (“**Target Location 5**”), residence of Mario GONZALEZ as described in Attachment A-5;
- f. Jose CHAVEZ telephone: 916-841-4806 (**TT1**), subscribed to Jose Zepeda, 3505 Condor Court, Carmichael, CA.
- g. Denis Zacarias PONCE’S telephone: 916-840-0486 (“**TT2**”), subscribed to Denis PONCE, 5717 Hillsdale Boulevard, Sacramento, CA;
- h. Mario Naranjo GONZALEZ’S telephone: 209-416-8448 (**TT3**), subscribed to GONZALEZ at 1412 Thomasnell Way, Ceres, CA.
- i. The following vehicles:
 - 1. 2018 Volkswagen sedan, white with CA license **8HKN876** (“**Target Vehicle 1**”), as described in Attachment A-6.
 - a. Registered to Jose Zepeda, 3505 Condor Court, Carmichael, CA
 - b. Driven by Jose CHAVEZ
 - 2. 2016 Honda sedan, grey with CA license **#8MHH330** (“**Target Vehicle 2**”), as described in Attachment A-7.
 - a. Registered to Jose M CHAVEZ, 3505 Condor Court, Carmichael, CA
 - b. Driven by Jose CHAVEZ
 - 3. 2020 Honda SUV, black with CA license **#8NKA590** (“**Target Vehicle 3**”), as described in Attachment A-8.
 - a. Registered to Jose M Zepeda or Nidia Chavez, 3505 Condor Court, Carmichael, CA
 - b. Driven by Jose CHAVEZ
 - 4. 2017 Honda Sedan, silver with CA license **#8KIV189** (“**Target Vehicle 4**”) as described in Attachment A-9.
 - a. Registered to Chavezzepeda Jose Manuel, 3505 Condor Court, Carmichael, CA
 - b. Parked at **Target Location 1**, Jose CHAVEZ residence.
 - 5. 2017 Honda Accord, grey with CA license **#7UWH104** (“**Target Vehicle 5**”), as described in Attachment A-10.
 - a. Registered to Denis Castillo, at 7987 Old Winding Way, Fair Oaks, CA
 - b. Driven by Denis PONCE

6. 2007 Saturn, grey with CA License #6WCJ577 (“**Target Vehicle 6**”) as described in Attachement A-11.
 - a. Registered to Registered to Denis Ponce Castillo, at 3825 Presidio St, Sacramento, CA
 - b. Driven by Denis PONCE
7. 2008 Toyota, black with CA License #81749E3 (“**Target Vehicle 7**”) as described in Attachement A-12.
 - a. Registered to Registered to Denis Ponce, at 3825 Presidio St, Sacramento, CA
 - b. Driven by Denis PONCE
8. 2021 Toyota Camry, white with CA license #8UHG728 (“**Target Vehicle 8**”), as described in Attachment A-13.
 - a. Registered to Mario Naranjo, at 1412 Thomasnell Way, Ceres, CA
 - b. Driven by Mario GONZALEZ
9. 2017 GMC, red truck with CA license #98560C2 (“**Target Vehicle 9**”), as described in Attachment A-14
 - a. Registered to Mario Naranjo, at 1412 Thomasnell Way, Ceres, CA
 - b. Driven by Mario GONZALEZ
10. 2007 Toyota, silver Tacoma, CA license # 36821B3 (“**Target Vehicle 10**”) as described in Attachment A-15
 - a. Registered to Jose CHAVEZ, at 3505 Condor Court, Carmichael, CA
 - b. Driven by Jose CHAVEZ
11. 1994 Jaguar, CA license # 3KST304, (“**Target Vehicle 11**”) as described in Attachment A-16
 - a. Registered to Jose CHAVEZ, at 3505 Condor Court, Carmichael, CA
 - b. Parked at **Target Location 3**
12. 1998 Ford, truck CA license #8V96908 (“**Target Vehicle 12**”) as described in Attachment A-17
 - a. Registered to Jose CHAVEZ, at 2533 Del Paso Blvd., Sacramento, CA
 - b. Driven by Jose CHAVEZ
 - c. Parked at **Target Location 3**

8. I request authority to search Target Locations 1 through 5 and Target Vehicles 1 through 12 for the items described in Attachment B.

Scope of Requested Criminal Complaint

9. This affidavit also supports an application for a criminal complaint and arrest warrants for:

- a) Jose Manuel CHAVEZ Zepeda
(Counts 1-2)
- b) Denis Zacarias PONCE Castillo
(Counts 1-2)

COUNT ONE – Conspiracy to Distribute and Possess with Intent to Distribute at least 500 grams of a Mixture and Substance containing Cocaine, in violation of 21 U.S.C. §§ 841(a)(1) and 846. (April 22, 2016 through the present)

COUNT TWO – Distribution of at least 500 grams of a Mixture and Substance containing Cocaine, in violation of 21 U.S.C. § 841(a)(1) (June 25, 2021).

Statement of Probable Cause

10. The United States Government, including FBI, has been investigating the drug trafficking activities of Jose Manuel CHAVEZ Zepeda, Denis Zacarias PONCE Castillo, and Mario Naranjo GONZALEZ since April 2016.

11. In 2016 and 2017, an FBI confidential human source (the “CHS”), provided information about Jose CHAVEZ.¹ The CHS had previously delivered multiple kilograms

¹ The CHS has a criminal history that includes a prior felony conviction for a drug trafficking offense. The CHS is cooperating with the FBI in the hopes of receiving assistance with the CHS’s immigration status. The FBI has been working with the CHS since April 2016. During that time, the FBI has not identified any issues of dishonesty with the CHS. Agents have been able to independently corroborate much of the information provided by the CHS related to the drug trafficking activities of CHAVEZ through surveillance, phone records, audio

(“kilos”) of cocaine to CHAVEZ’s sub-dealers in the Sacramento, California (“CA”) area.

The CHS also provided the following information:

a) CHAVEZ’s cocaine Source of Supply (hereinafter “SOS”) is an individual he called “Compadre,” who resides in Mexico. The CHS believes CHAVEZ and Compadre are very close. Compadre is connected to the Cartel Jalisco Nuevo Generacion, or “CJNG.” The cocaine the CHS would deliver would be marked with the “NG” (for Nuevo Generacion) stamp on them.

b) Compadre arranges for the cocaine to be smuggled into the United States and transported to Los Angeles, CA. The cocaine is smuggled into the United States in semi-trucks transporting other goods. Once the cocaine reaches Los Angeles, it is then loaded into smaller Nissan trucks and driven to an individual known as “Joto” in Ceres, CA. Sometimes “Joto” would drive to southern CA to pick up the cocaine. The CHS positively identified “Joto” as Mario Naranjo GONZALEZ via DMV photograph.

c) GONZALES drove a white Ford truck with a false compartment installed in it. The CHS ran special errands for CHAVEZ and delivered \$230,000, \$100,000, and \$80,000 cash, all on separate occasions, to GONZALEZ, who was also storing cocaine on behalf of CHAVEZ (as well as delivering narcotic proceeds back to the SOS). The CHS stated the \$230,000 was the proceeds from one week of narcotic sales. GONZALEZ stored the money he received in his garage until he was ready to take it down to Mexico.

d) GONZALEZ previously told the CHS that he stored the narcotics (for CHAVEZ) at his (GONZALEZ’s) aunt’s house.

recordings, and other information. I am not aware of the CHS providing false or misleading information during this investigation. For these reasons, I believe the information provided by the CHS to be reliable.

e) The CHS stated that when someone in Sacramento, CA needed cocaine, the CHS would pick it up from GONZALEZ and deliver it to the person who needed it.

f) In July 2021, the CHS stated that Compadre used to supply GONZALEZ with cocaine and then GONZALEZ would be the SOS for CHAVEZ. At some point, CHAVEZ went directly to Compadre and started getting cocaine directly from him. This upset GONZALEZ. Compadre told CHAVEZ and GONZALEZ that they needed to work together. After that, CHAVEZ and GONZALEZ ordered their cocaine from Compadre together and made their payments together (bundling narcotics orders and payments together).

g) CHAVEZ would sell kilos of cocaine for \$28,000 - \$30,000.

h) One of CHAVEZ's larger sub-dealers was a Central American guy known as "El Ciego," "Casi Miro," or "El Tuerto," who works at a mechanic shop. The CHS would deliver cocaine to "El Ciego" at the mechanic shop where he works. The CHS had previously communicated with "El Ciego" on telephone number 916-821-5489 (hereinafter "x5489") but did not believe that the number was still being used. In May 2021, the CHS positively identified "El Ciego" as Denis Zacarias PONCE Castillo using a social media photograph.

i) The CHS believes CHAVEZ stores the proceeds from his narcotic sales in his bedroom closet at his house. CHAVEZ uses a shrink wrapper in his room to shrink wrap the money into bundles of \$100,000.

j) As of June 2021, the CHS communicated with CHAVEZ on telephone number 916-841-4806 (hereinafter "TT1").

k) CHAVEZ currently owns and operates La Victoria Supermercado, located at 2533 Del Paso Boulevard, Sacramento, CA (**Target Location 2**). CHAVEZ uses this grocery store to launder proceeds from his narcotic sales. The CHS has direct knowledge of the business dealings inside La Victoria Supermercado. CHAVEZ is believed to be

laundering narcotics sale proceeds (through money remitters, bulk cash deposits, and business proceeds) to affiliates in Mexico.

Arrangements for the Purchase of Cocaine on June 25, 2021

12. According to the CHS, on June 8, 2021, CHAVEZ spoke with the CHS in person. CHAVEZ offered to sell the CHS a half kilogram or quarter kilogram of cocaine as someone else had requested a half kilogram as well.

13. On June 15, 2021, the CHS told the FBI that the CHS met with CHAVEZ in November 2020 or December 2020 at La Victoria Supermercado. PONCE arrived at the location and gave an unknown amount of money to CHAVEZ. CHAVEZ later told the CHS that PONCE, whom CHAVEZ trusted a great deal, was the “stash pad” manager (for their cocaine).

14. According to the CHS, on June 17, 2021, the CHS went to La Victoria Supermercado to meet with CHAVEZ. CHAVEZ exited the market and entered his truck where the CHS and CHAVEZ discussed the purchase of cocaine. CHAVEZ stated he was willing to sell the CHS half a kilogram of cocaine. CHS would be paying \$7,000.00 for a quarter kilogram of cocaine and owing CHAVEZ for the remaining quarter kilogram.

15. On June 24, 2021, law enforcement officers monitored and recorded the CHS engaging in narcotics related meeting with CHAVEZ and PONCE during which the CHS discussed the purchase of cocaine. The CHS met with CHAVEZ and PONCE at La Victoria Supermercado (**Target Location 2**). The CHS, CHAVEZ and PONCE discussed the purchase of cocaine in the CHAVEZ’s office inside **Target Location 2**. CHAVEZ informed PONCE that the CHS was interested in purchasing half a kilogram of cocaine. PONCE then stated they would need to call the other guy. PONCE then placed a telephone

call and spoke with an unidentified person for approximately 2 to 3 minutes. At the conclusion of the telephone call, PONCE said it was good. Based off the series of events, the CHS believed that PONCE had called the other guy and confirmed that he wanted the other half kilogram of cocaine. The CHS was instructed to call PONCE on 916-840-0486 (“TT2”) on June 25, 2021 at around 7:00am and he would sell him the half kilogram of cocaine. PONCE provided the CHS with his address, 1051 Fulton Avenue in Sacramento, CA, as the location to meet him in the morning to pick up the cocaine.

Controlled Purchase of 508.5 Grams of Cocaine from CHAVEZ and PONCE on June 25,

2021

16. On June 25, 2021, agents established physical surveillance at his residence at 2480 Larkspur Lane, Sacramento, California (**Target Location 4**). Agents observed PONCE leave the condominium complex and after some stops arrived at 4158 Scranton Circle, Sacramento, CA. At the time, 4158 Scranton Circle was the known residence of CHAVEZ. **Target Vehicles 2, 3 and 4** were observed outside of the residence. Agents witnessed CHAVEZ park **Target Vehicle 2** in front of the residence and enter the residence. PONCE later exited the residence. The CHS placed a recorded call to PONCE after PONCE was witnessed exiting the residence. PONCE immediately responded, in Spanish, with “I am now ready.”² The CHS and PONCE then agreed to meet at **Target Location 2**. Prior to the CHS’s arrival, officers searched the CHS for contraband with negative results, and outfitted the CHS with a recorder and transmitter.

² I am a native Spanish speaker. I reviewed the Spanish language recording and translated it into English.

17. The CHS received an incoming call from PONCE's telephone number, **TT2**. PONCE asked for the CHS's estimated time of arrival. The CHS and PONCE exchanged the following text messages:

PONCE: Estoy Afuera (I am outside)

CHS: Aqui estoy yo en el carro blanco. Que carro traes tu? (I am here in the white car. What car are you in?)

Agents observed PONCE approach the CHS's driver side window. PONCE handed a brown bag to the CHS. PONCE in exchange, received the \$7,000.00 from the CHS.

18. After the meeting, the CHS immediately met with agents and turned a brown bag containing the cocaine and the recording devices. The cocaine was subsequently analyzed by the DEA Laboratory, where it tested positive for cocaine and was found to weigh 508.5 grams net weight.

Cocaine Debt Payment of \$4,000 to CHAVEZ on July 16, 2021

19. On July 16, 2021, law enforcement officers monitored and recorded the CHS engaging in a narcotics related meeting at La Victoria Supermercado (**Target Location 2**), where the CHS had planned to meet with CHAVEZ to conduct a partial payment for the cocaine purchased on June 25, 2021. A detective observed a silver Toyota Tacoma with CA license plate 36821B3 ("**Target Vehicle 10**") (registered to CHAVEZ) in the parking lot of La Victoria Supermercado. A detective observed **Target Vehicle 7** (registered to PONCE) parked in the rear of 2566 Rio Linda Boulevard, Sacramento, CA (**Target Location 3**). The residence at **Target Location 3** is located across the street from the rear of La Victoria Supermercado. As further explained below, **Target Location 3** is believed to be controlled by CHAVEZ and to be a drug stash location. When the CHS arrived at the Market,

CHAVEZ was exchanging checks for a long line of customers. The CHS had to wait a while to talk to CHAVEZ. While the CHS was waiting, PONCE walked into the Market unexpectedly. Once CHAVEZ was done with the customers, CHAVEZ, PONCE and the CHS entered the office together. The CHS observed PONCE enter the office holding small pieces of paper and, according to the CHS, PONCE stated “with this we are going to be good.” The CHS then CHAVEZ and PONCE discuss a new delivery of cocaine and CHAVEZ encouraged the CHS to purchase more (cocaine) from them. CHAVEZ instructed PONCE to pick up two (presumably kilos of cocaine) as soon as possible. CHAVEZ encouraged PONCE to leave right away and PONCE stated he was tired. CHAVEZ told PONCE to go first thing in the morning. After PONCE left the office, the CHS told CHAVEZ he only had \$4,000.00 as a payment. CHAVEZ took the money from the CHS, counted it, and stated it was not a problem. CHAVEZ told the CHS that “Joto” (GONZALEZ) had sold his food truck, purchased a bar, called La Huacana, but had since sold it.

20. I reviewed the recording on July 16, 2021, in which the CHS and CHAVEZ spoke in Spanish. The following is only a summary of what I observed and heard in the recording. The CHS handed CHAVEZ the money and CHAVEZ asked the CHS if they liked it. CHAVEZ asked if the CHS noticed the marking, and the CHS stated he saw the number “68” on the packaging. CHAVEZ stated “I only did this” and made a gesture with his hands as if he was splitting something in half. The CHS asked if the number (on the packaging) was in reference to the purity of the cocaine. CHAVEZ stated no, and that the cocaine he received was assigned a number. He further explained that if there was ever an issue with the cocaine, CHAVEZ would reference the number on the cocaine. He said that

everyone who has a “line” has numbers assigned to the cocaine they manage. CHAVEZ mentioned that on the last shipment, he had to return one, referring to a kilogram of cocaine. CHAVEZ stated he spoke to “Compadre” about the cocaine. CHAVEZ made statements regarding the “beauty” and pureness of the cocaine. He also stated that he himself split it. CHAVEZ stated he gave the cocaine to the CHS as he had received it aside from splitting it. CHAVEZ stated he never splits them (referring to the kilogram packages of cocaine) and that he typically always sells them whole. CHAVEZ encouraged the CHS to purchase a whole kilo of cocaine verses the half. CHAVEZ stated the CHS would make more money that way. After the meeting, the CHS immediately met with agents to turn over the recording devices. Based on my training and experience, I believe that CHAVEZ was referring to a kilogram package of cocaine, numbered “68,” which he split in half to sell to the half kilogram to the CHS on June 25, 2021.

PONCE Travels to the Area of GONZALEZ’s Residence (Target Location 5) on July 17, 2021, Apparently to Pick Up Two Kilograms of Cocaine at CHAVEZ’s Direction

21. The next day, on July 17, 2021 (the next day), geolocation data for TT2 (PONCE) indicates TT2 traveled to Ceres, CA. Geolocation data on TT2 indicates TT2 was in the proximate area of 1412 Thomasnell Way, Ceres CA (**Target Location 5**), GONZALEZ’s address per public database inquiries. Geolocation data on TT2 indicates TT2 was in Ceres, CA for a short period of time (from approximately 3:29pm to 3:44pm) prior to returning to the Sacramento, CA area. Based on my training, experience, and knowledge of this investigation, I believe PONCE likely traveled to Ceres to pick up two kilograms of cocaine from GONZALEZ at CHAVEZ’s direction.

22. On July 20, 2021, agents obtained the CA Secretary of State electronic filing for La Huacana, Inc. In summary, La Huacana, Inc. is a night club and bar, located at 101 E Glenn Avenue #A, Modesto, CA 95358. The filing date was July 24, 2020, with the Chief Executive Officer, Secretary, Chief Financial Officer, Director, and Agent of Service of Process all listed as Mario Naranjo GONZALEZ at 1412 Thomasnell Way, Ceres, CA (**Target Location 5**). The electronic signature listed Mario N GONZALEZ.

23. A public records database inquiry on GONZALEZ revealed a possible telephone number of 209-416-8448 (**TT3**). Subscriber information showed **TT3** listed as subscribed to Mario GONZALEZ, located at 1412 Thomasnell Way, Ceres, CA. Toll analysis on **TT1** (**CHAVEZ**) revealed communication with **TT3** (GONZALEZ) on May 6, May 9, May 10, and June 17, July 8, July 14 through July 16, and July 28 (all of 2021).³ Agents later obtained a WhatsApp pen register (starting on August 14, 2021), which shows dozens of additional communications between **TT1** and **TT3**.

Cocaine Debt Payment of \$3,000 to CHAVEZ and PONCE on July 22, 2021

24. On July 22, 2021, law enforcement officers monitored and recorded the CHS engaging in a narcotics related meeting at La Victoria Supermercado (**Target Location 2**), where the CHS had planned to meet with CHAVEZ for the final payment of the cocaine purchased on June 25, 2021. The following information was provided by the CHS when the CHS was debriefed after the payment to CHAVEZ was completed.⁴ Once inside of the market,

³ On July 16, 2021, CHAVEZ told the CHS that he had not been in communication with GONZALEZ for a while. Based on these toll communication and PONCE's trip to Ceres on July 17, 2021, apparently to pick up two kilograms of cocaine from GONZALEZ, I believe CHAVEZ was misleading the CHS about his recent communications with GONZALEZ.

⁴ Due to the rustling of the recording device, some of the recording is difficult to understand.

CHAVEZ and the CHS entered the office inside the market. The CHS noticed PONCE sitting inside of the office. The CHS handed CHAVEZ \$3,000.00. CHAVEZ asked the CHS when he would be purchasing more and stated he was ready to supply the CHS. CHAVEZ stated he was receiving approximately five to six (kilograms) each delivery, which the CHS understood to be weekly. CHAVEZ further stated the cocaine he was getting was good quality. The CHS left when PONCE got up to leave and said goodbye to both CHAVEZ and the CHS. After the meeting, a detective observed the CHS greet PONCE in the parking lot. PONCE then accessed **Target Vehicle 5**, walked to the rear of the residence located at 2556 Rio Linda Boulevard (**Target Location 3**), opened the gate, and got into **Target Vehicle 6** and moved it off of the property through the same gate. PONCE then exited **Target Vehicle 6**, closed the gate, returned to **Target Vehicle 6**, and departed.

Additional Evidence of CHAVEZ's and GONZALEZ's Joint Narcotics Trafficking

Activities

25. In June 2021, agents conducted law enforcement database inquiries with the Department of Homeland Security (hereinafter "DHS") relating to known vehicles registered to CHAVEZ. The license plate inquiries revealed the following:

- a) CA license plate 36821B3 crossed the U.S. / Mexico border on February 27, 2021 and March 24, 2021. The operators of the vehicle during those crossings were Katie Vanesa CAMPOS (February 27, 2021) and Uriel DELREAL (March 24, 2021).

- b) CA license plate 8KIV189 (**Target Vehicle 4**) crossed the U.S. / Mexico border on March 27, 2021 and April 6, 2021. The operator of the vehicle during those crossings was Celeste CAMPOS.
26. Further law enforcement database inquiries with DHS on K. CAMPOS, C. CAMPOS, and DELREAL revealed the following:
- a) DELREAL crossed the U.S. / Mexico border approximately 170 times in 2021. Of specific interest, DELREAL crossed the U.S. / Mexico border on February 16, 2021 in a vehicle with CA license plate 8T83538. A DMV inquiry on CA license plate 8T83538 revealed the vehicle was a 2010 Ford truck previously registered to Mario Naranjo, located at 1412 Thomasnell Way, Ceres, CA (**Target Location 5**). There was a release of liability on the truck dated November 26, 2019, with the new registered owner listed as Jose Lopez Chavez, located at 2533 Del Paso Boulevard (the address for La Victoria Supermercado, **Target Location 2**).
- b) C. CAMPOS crossed the U.S. / Mexico border approximately 50 times in 2021.
- c) K. CAMPOS crossed the U.S. / Mexico border approximately 85 times in 2021.
- d) It should also be noted that DELREAL, C. CAMPOS, and K. CAMPOS were listed as both vehicle operators and sometimes passengers while one of the others were driving. For example, on March 26, 2021, C. CAMPOS was operating a vehicle that crossed the U.S. / Mexico border, and DELREAL was a passenger in the vehicle.
- e) A law enforcement database inquiry on CA license plate 8T83538 revealed it was a white Ford F-150.

f) Based on my training, experience, and knowledge of the investigation, I believe the 2010 Ford F-150 with CA license plate 8T83538 is likely the vehicle containing a hidden compartment that was described by the CHS. I the previous registered owner, Mario Naranjo, is GONZALEZ. Additionally, DMV records reveal that the current registered owner, Jose Lopez Chavez is CHAVEZ. Based on the totality of information, I believe that GONZALEZ, DELREAL, C. CAMPOS, and K. CAMPOS are involved in this drug trafficking organization (“DTO”).

27. On July 27, 2021, court-authorized geolocation data for **TT3** (GONZALEZ) indicates **TT3** was in the area of La Victoria Supermercado (**Target Location 2**). At around 5:35 p.m., surveillance observed GONZALEZ’s 2017 GMC truck with CA license plate 98560C2 in the parking lot of La Victoria Supermercado. Court-authorized geolocation data for **TT1** (CHAVEZ) indicates **TT1** was also in the area of La Victoria Supermercado. Geolocation data for **TT3** indicates **TT3** was in the area for approximately 2.5 hours prior to returning to the area of GONZALEZ’s residence in Ceres (**Target Location 5**). A law enforcement database inquiry on CA license plate 98560C2 revealed the vehicle had scanned in the Sacramento, CA at 5:20 p.m. near La Victoria Supermercado, and then again at 10:36 p.m. at the same prior scan location (while geolocation for x8448 was in Ceres, CA). Geolocation data for **TT1** indicates **TT1** was in the same proximate area as the license plate scan at 10:36 p.m. (indicating that CHAVEZ likely had possession and control of GONZALEZ’s vehicle). At approximately 10:48 p.m., geolocation data for **TT3** (GONZALEZ) indicates **TT3** travelled to Vancouver, Washington (“WA”), arriving in the mid-afternoon on July 28, 2021. Geolocation data for **TT3** indicates **TT3** remained in

Vancouver, WA for approximately 6 hours prior to returning to the area of GONZALEZ's residence (on July 29, 2021). On July 29, 2021 at around 3:13p.m., a law enforcement database inquiry on CA license plate 8UHG728 (registered to GONZALEZ) (**Target Vehicle 8**) revealed the vehicle scanned in the same proximately location as geolocation data for **TT3** (while returning to Ceres, CA). Based on the foregoing, I believe GONZALEZ traveled to Vancouver, WA in **Target Vehicle 8**.

28. On September 8, 2021, GONZALEZ traveled to Vancouver, WA, where he remained for approximately 3.5 hours, prior to returning to the Ceres, CA area (on September 9, 2021).

- a) A WA Narcotic Task Force observed GONZALEZ arrive in an apartment complex located at 2508 NE 138th Avenue, Vancouver, WA at around 7:08 p.m. He was driving **Target Vehicle 8** and was the sole occupant of the vehicle. GONZALEZ carried a white plastic shopping bag with items inside resembling Tupperware containers into apartment A8. Local law enforcement database inquiries revealed Salvador Campos-Torres, Katherine Campos-Torres, Eduardo Campos-Torres, and Rafael Campos were associated with apartment A8. During the surveillance, several Hispanic male adults were observed entering the apartment (with GONZALEZ inside) carrying backpacks. All of their stay was short in nature, and when they exited the apartment, they were no longer carrying backpacks. GONZALEZ was observed carrying a backpack inside the apartment during the surveillance, but it appeared to be empty, or close to empty (based off the shape and way the backpack was being carried). When GONZALEZ left the apartment, the backpack appeared to be partially full.

b) Per the Clark / Vancouver Regional Drug Task Force, Rafael Campos is married to, or in a relationship with, Isela Campos-Gonzalez. Isela Campos-Gonzalez's mother is Marisol Torres Cervantes. On April 17, 2020, Oregon State Police conducted a vehicle stop on a 2019 Nissan Rogue registered to Isela Campos-Gonzalez. The driver and sole occupant of the vehicle was Marisol Torres Cervantes. A consent search of the vehicle revealed a manufactured floor compartment and approximately 7 pounds of cocaine and 4.5 grams of heroin. Insurance identification cards located inside the vehicle showed that Isela Campos-Gonzalez and Rafael Campos-Barajas were insured on the vehicle.

29. On October 14, 2021, court-authorized geolocation data for **TT3** (GONZALEZ) indicates **TT3** traveled to Vancouver, WA, where **TT3** remained for approximately four hours, prior to returning to the Ceres, CA area (on October 15, 2021). A Washington Narcotic Task Force observed GONZALEZ arrive in an apartment complex located at 2508 NE 138th Avenue, Vancouver, WA at around 3:50 p.m., driving **Target Vehicle 8**. GONZALEZ carried a pink shopping bag with items inside into an apartment. During the surveillance, at least one Hispanic male adult was observed entering the apartment (with GONZALEZ inside) carrying a backpack. The stay was short in nature, and when he exited the apartment, he was no longer carrying a backpack.

30. On March 12, 2022, at around 11:05 am, geolocation data for **TT3** (GONZALEZ) indicates **TT3** left the area of **Target Location 5**(GONZALEZ's residence in Ceres), and traveled to Sacramento, CA, arriving between 12:20 p.m. and 12:35 p.m. at a location near **Target Location 1** (CHAVEZ's residence). Geolocation data for **TT1** (CHAVEZ) indicates **TT1** was in the area of **Target Location 1** at around the same time. Surveillance

units witnessed PONCE arrive at **Target Location 1**, and GONZALEZ arrived shortly after. About six minutes after he arrived, GONZALEZ departed **Target Location 1**, driving **Target Vehicle 9**. Less than an hour later, detectives witnessed CHAVEZ, PONCE and GONZALEZ gathering together in a restaurant parking lot in Sacramento. They left the location, with GONZALEZ driving **Target Vehicle 9**, and CHAVEZ driving **Target Vehicle 1** with PONCE as a passenger, and returned to **Target Location 1** (CHAVEZ's residence). About 10 minutes later, GONZALEZ and PONCE each left in their respective vehicles (**Target Vehicles 9 and 6**).

Money seizure from Mario Naranjo GONZALEZ on October 15, 2021

31. On October 15, 2021, at 11:54 a.m., the Sacramento County Sheriff's Office conducted a traffic enforcement stop on **Target Vehicle 8**. The driver and sole occupant of the vehicle was identified as GONZALEZ. A canine, trained in the detection of narcotics, positively alerted on the vehicle. A subsequent search of the vehicle revealed two bundles of cash, wrapped in green saranwrap, hidden underneath the upholstery of the driver's front seat rear backing, as well as ten additional bundles of cash, wrapped in green saranwrap, hidden underneath the upholstery of the passenger's front seat rear backing. GONZALEZ, who was detained after the canine narcotic alert, was escorted to stand near the marked patrol vehicle, unhandcuffed. GONZALEZ initially denied knowing the money was in the vehicle, or that it belonged to him. GONZALEZ stated he was coming from Sacramento, CA and driving to Modesto, CA. Upon further questioning, GONZALEZ stated that he was a money courier and that he would make \$1,000 to make money courier trips from Sacramento, CA to Modesto, CA. GONZALEZ stated that his wife was also a money courier. GONZALEZ stated that his telephone number was **TT3**. A deputy observed that

GONZALEZ had two Android phones in his vehicle at the time of the stop. GONZALEZ was released from the scene, and the bundles of cash were seized. A subsequent search and processing of the bundles of cash revealed there was \$79,470 in total.

a) Based on my training, experience, and knowledge of the investigation, I know “short stay” traffic is an indication of narcotic sales. I believe GONZALEZ traveled to Vancouver, WA with an undisclosed type and quantity of narcotics, and received \$79,470 in cash in exchange for the narcotics. GONZALEZ then concealed the cash in the seats to avoid detection and apprehension by law enforcement, prior to traveling toward the Sacramento, CA area.

b) Prior toll analysis and WhatsApp pen register analysis identified one of GONZALEZ’s top contact numbers as 209-918-0164 (hereinafter “x0164”). A law enforcement financial database inquiry on x0164 revealed the number was associated with Griselda Guadalupe Orozco NARANJO at 1412 Thomasnell Way, Ceres, CA. NARANJO is believed to be the wife of GONZALEZ.

Money seizure from C. CAMPOS and Julio VEGA on January 27, 2022

32. As discussed above, law enforcement checks conducted by DHS revealed numerous U.S. /Mexico border crossings in vehicles belonging to CHAVEZ and GONZALEZ to include; 2018 Volkswagen license plate 8HKN876 (**Target Vehicle 1**), 2017 GMC license plate 98560C2, and 2017 Honda sedan 8KIV189 (**Target Vehicle 4**). Border crossings revealed that at various times, the drivers and passengers were K. CAMPOS, DELREAL, and C. CAMPOS.

33. C. CAMPOS (utilizing telephone number 619-870-7147, “x7147”), K. CAMPOS, and DELREAL have been identified in the investigation as suspected money couriers residing in southern CA and in Mexico for the DTO.

34. A law enforcement database inquiry with DHS on Mexico license plate WFK-930-A revealed it crossed the Otay Mesa POE on January 24, 2022, at 2:37 p.m., one minute before C. CAMPOS crossed the border. The driver, Julio Cesar Sanchez VEGA had previously crossed the U.S. / Mexico border with C. CAMPOS on November 24, 2021.

35. Pen register data on **TT1** (CHAVEZ) indicates **TT1** was in contact with **TT3** (GONZALEZ) on January 24, 2022 at 9:25 p.m.

36. On January 25, 2022, geolocation data on x7147 (C. CAMPOS) indicated x7147 began traveling northbound on Highway 99 at around 11:00 a.m. At around 2:15 p.m., the Modesto Police Department conducted a traffic enforcement stop on the blue Volkswagen Jetta with Mexico license plate WFK-930-A. The two occupants were driver VEGA (identified via B1/B2 Visa) and passenger C. CAMPOS (CA driver’s license). VEGA related he had just rented the Jetta in Mexico (and showed a rental agreement in support of his statement) and stated he was traveling to Sacramento, CA to visit his father’s good friend. A police canine, trained in the detection of narcotics, positively alerted on the trunk of the vehicle. A subsequent search of the vehicle was met with negative results, and VEGA and C. CAMPOS were released from the scene.

37. Detectives conducted surveillance on VEGA and C. CAMPOS. At around 4:15 p.m., detectives observed the blue Volkswagen Jetta with Mexico license plate WFK-930-A pull into the La Victoria Supermercado parking lot (**Target Location 2**). VEGA and C.

CAMPOS exited the blue Volkswagen Jetta with Mexico license plate WFK-930-A and entered the store. At around 5:15 p.m. surveillance was terminated.

38. Geolocation data on **TT1** (CHAVEZ) indicates **TT1** was at the store when VEGA and C. CAMPOS arrived. At around 5:48 p.m., geolocation data for x7147 indicates x7147 left the store and went to a hotel near I-5 and Richards Boulevard in Sacramento, CA. At around 8:19 p.m., geolocation data for x7147 indicates x7147 traveled to the area of Fair Oaks Boulevard and Howe Avenue in Sacramento, CA, where it remained until around 10:05 p.m. Geolocation data on x7147 indicates x7147 traveled to the area of CHAVEZ's residence (**Target Location 1**) from 10:35 p.m. to 10:50 p.m., prior to traveling back to the area of I-5 and Richards Boulevard in Sacramento, CA. Geolocation data on **TT1** (CHAVEZ) indicates **TT1** left **Target Location 2** at around 8:19 p.m. and responded to the area of Fair Oaks Boulevard and Howe Avenue in Sacramento, CA, where it remained until around 10:05 p.m. Geolocation data on **TT1** indicates **TT1** traveled to the area of CHAVEZ's residence (**Target Location 1**), arriving at around 10:35 p.m., where it remained for the evening.

39. On January 26, 2022 at around 1:57 p.m., geolocation data for x7147 (C. CAMPOS) indicates x7147 traveled from the Sacramento, CA area to the area of **Target Location 5** (GONZALEZ's residence in Ceres), arriving at around 3:28 p.m. Geolocation data on x7147 indicates x7147 remained in the area until around 4:29 p.m. prior to traveling to the Bakersfield, CA area (arriving at around 8:00 p.m.) Geolocation data for x7147 indicates x7147 remained in Bakersfield until January 27, 2022.

40. On January 27, 2022 at around 9:36 a.m., geolocation data for x7147 (C. CAMPOS) indicates x7147 traveled from Bakersfield, CA to San Diego, CA. At around 2:49 p.m., the

San Diego County Sheriff's Department conducted a traffic enforcement stop on the blue Volkswagen Jetta with Mexico license plate WFK-930-A. VEGA was operating the vehicle and C. CAMPOS was a passenger in the vehicle. A consent search of VEGA and the vehicle was conducted, and a total of \$71,280 was located. Per the San Diego Sheriff's Department, VEGA stated a portion of the money was proceeds from him selling a vehicle. C. CAMPOS did not have an explanation for the money inside the vehicle. Based on the way the money was packaged (some held with rubber bands, and some plastic sealed) and where it was located, as well as a canine trained in the detection of narcotics alerting on an area where money was located, the San Diego Sheriff's Department Deputy believed the money was proceeds from narcotic trafficking.

Pen Register Data

41. Pen register analysis on **TT1(CHAVEZ)** indicates **TT1** has been in contact with **TT3** (GONZALEZ) over 20 times between May 6, 2021 and March 3, 2022. Pen register analysis on **TT1** (CHAVEZ) indicates **TT1** has been in contact with **TT2** (PONCE) over 50 times between February 3, 2022 and March 5, 2022. Pen register analysis on **TT2** (PONCE) indicates no communication with **TT3** (GONZALEZ).

Additional Surveillance of Target Location 1

42. On January 14, 2022, surveillance was conducted on 3505 Condor Court, Carmichael, CA (**Target Location 1**). Agents observed a white Volkswagen, license plate 8HKN876 (**Target Vehicle 1**) registered to Jose Zepeda and a black Honda, license plate 8NKA590 (**Target Vehicle 3**). The registered address for both vehicles is listed as 3505 Condor Ct., Carmichael, CA. In March 2022, law enforcement checks conducted on CHAVEZ, listed his current address as 3505 Condor Ct., Carmichael, CA.

43. On February 2, 2022, surveillance was conducted on 3505 Condor Court, Carmichael, CA (**Target Location 1**). Agents observed a black Honda, license plate 8NKA590 (**Target Vehicle 3**) and white Honda sedan license plate 8KIV189 (**Target Vehicle 4**). Agents observed CHAVEZ leave the front door area of the residence and enter **Target Vehicle 3**.

44. On March 7, 2022, surveillance was conducted at 3505 Condor Court, Carmichael, CA (**Target Location 1**). Detectives witnessed PONCE arrive at residence driving **Target Vehicle 6**. PONCE departed the **Target Location 1** and later detectives witnessed **Target Vehicle 1** leave from the garage of the residence. The sole occupant of **Target Vehicle 1** was identified as CHAVEZ. After departing the residence, CHAVEZ was witnessed arriving at La Victoria Supermercado (**Target Location 2**).

45. Based on my training, experience, and knowledge of this investigation, I believe CHAVEZ resides at **Target Location 1** and likely uses it as a stash location for illegal drugs and drug proceeds. Agents believe Nidia Chavez, believed to be CHAVEZ's wife, may also live at **Target Location 1** based on surveillance observations of vehicles co-registered to CHAVEZ and Nidia Chavez in the driveway of the residence. Agents believe there may be juveniles living at **Target Location 1** based on the surveillance observation of CHAVEZ leaving the residence with two juveniles on February 4, 2022. Agents have not observed any indication of anyone else living at **Target Location 1**.

Target Location 3: 2556 Rio Linda, Sacramento, CA

46. As noted above, the residence at **Target Location 3** is located across the street from the rear of La Victoria Supermercado (**Target Location 2**). **Target location 2** and **3** are separated by an alley way and **Target Location 3** has a black iron gate surrounding the

property. On March 9, 2022, Sacramento Municipal Utility District (SMUD) revealed utilities were listed under the name of Maria Estela DELGADO. It is unknown what relationship DELGADO has with CHAVEZ or PONCE. On March 12, 2022, DELGADO was observed at the residence of **Target Location 3**.

47. On June 3, 2021, during a surveillance operation, detectives witnessed PONCE exit La Victoria Supermercado (**Target Location 2**) and drive **Target Vehicle 6** to the rear of the supermarket. Detectives lost sight of **Target Vehicle 6** briefly but observed PONCE closing the metal gate running across the driveway of **Target Location 3**. **Target Vehicle 6** was located in the yard behind the gate. Detectives observed two additional vehicles behind the gate: **Target Vehicle 5** (used by PONCE) and **Target Vehicle 11**(registered to Jose CHAVEZ, address 3505 Condor Court, Carmichael, CA), parked in the yard of **Target Location 3**.

48. As noted above, on July 16, 2021, surveillance saw **Target Vehicle 7** (registered to PONCE) parked at **Target Location 3** during the surveillance related to the CHS's payment of \$4,000 in drug proceeds to CHAVEZ at La Victoria Supermercado (**Target Location 2**). While the CHS was meeting with CHAVEZ to pay the drug proceeds, PONCE came into **Target Location 2** and discussed drug business with CHAVEZ. Similarly, on July 22, after the CHS met with CHAVEZ and PONCE in the office at **Target Location 2** to pay CHAVEZ \$3,000 in drug proceeds, PONCE was observed walking to **Target Location 3**, where he got into **Target Vehicle 6**.

49. On February 4, 2022, surveillance units witnessed PONCE arrive at **Target Location 2** in **Target Vehicle 6**. Shortly after, PONCE was seen using a key to enter the gate to

Target Location 3. PONCE was seen walking inside the gated area of the property, as **Target Vehicle 6** blocked the driveway of the residence.

50. On March 9, 2022, surveillance units witnessed a “Tacos La Victoria” taco truck stationed inside the secured yard of the residence at **Target Location 3.** On March 12, 2022, detectives witnessed the same taco truck stationed in the parking lot of **Target Location 2** (La Victoria Supermercado). Surveillance units also witnessed **Target Vehicle 11** (expired registration; registered to CHAVEZ from 12/14/2017 through 12/14/2018) parked inside of the residence of **Target Location 3.** Detectives also witnessed **Target Vehicle 12** (a white box truck, 1998 Ford, CA license plate 8V96908, with current registration dates of 03/31/22 through 03/31/2023, registered to CHAVEZ at **Target Location 2.** Based on my training and experience and the totality of the evidence, I believe **Target Location 3** is controlled by CHAVEZ and that CHAVEZ is likely using **Target Location 3** as a drug stash location and/or that **Target Location 3** contains evidence of CHAVEZ’s and PONCE’s drug trafficking activities.⁵

Target Location 4: 2480 Larkspur Lane, #176, Sacramento, CA

51. Records produced by Facebook in response to a search warrant for PONCE’s Facebook account listed several IP addresses used to log into the account. A subpoena for one of these IP addresses, IP Address 99.21. 146.78, revealed subscriber address information to 2480 Larkspur Lane #176, Sacramento, CA, which is a condominium

⁵ In 2018, the CHS reported that the trailer, or the location where the trailer is stored, that CHAVEZ has at La Victoria Market (**Target Location 2**) may be the place where CHAVEZ is storing his drugs. The CHS further stated that CHAVEZ had a girlfriend who used to stash drugs at CHAVEZ’S direction.

Agents have not observed any indication of anyone else living at **Target Location 3**, other than Maria Estela DELGADO, as described above.

address managed by Timberlake Owners Association. Agents requested information regarding 2480 Larkspur Lane #176, Sacramento, CA, and staff disclosed that the assigned parking space for the address was space 59. On January 14, 2022, agents observed PONCE's vehicle, **Target Vehicle 5**, parked in assigned parking space 59. On March 2, 2022, agents observed another of PONCE's vehicles, **Target Vehicle 6**, parked in parking space 59.

52. On March 7, 2022, agents attempted to conduct an undercover DoorDash at #176. The agent traveled up the single-entry staircase to #175 and #176. The single staircase is the only entry and exit point for the occupants. After several unsuccessful knocks at #176, the agent knocked at #175, an unknown female opened the door and stated two males resided in #176.⁶ Surveillance continued after the agent departed the location. Later in the day, detectives witnessed PONCE walk down the staircase of #175 and #176. PONCE entered **Target Vehicle 6** parked in parking space 59 whereupon he exited the condominium. PONCE drove his vehicle to 3505 Condor CT., Sacramento, CA (**Target Location 1**), where he exited and entered the residence.

53. On March 12, 2022, surveillance units witnessed PONCE arrive at **Target Location 4** and park in space 59. PONCE was later seen exiting the stairway that led to his apartment carrying a laundry basket full of clothes and driving to a laundromat.

54. Based on the above information and totality of the investigation, I believe PONCE currently resides at 2480 Larkspur Lane #176, Sacramento, CA (**Target Location 4**).

⁶ Saman Dehghani Mohammadi is listed as the subscriber for the internet service provided to **Target Location 4**. Agents do not know whether Mohammadi is the other male whom the resident of #175 stated lives at **Target Location 4**.

Target Location 5: 1412 Thomasnell Way, Ceres, CA

55. On March 1, 2022, law enforcement checks conducted on Mario GONZALEZ revealed address 1412 Thomasnell Way, Ceres, CA (**Target Location 5**) as a primary address. Agents believe based on a law enforcement financial records database inquiry that Griselda Guadalupe Orozco NARANJO, believed to be GONZALEZ's wife (whom GONZALEZ told law enforcement was also a money courier during the October 15, 2021 traffic stop described above), likely also lives at **Target Location 5**. Agents have not observed any indication of anyone else living at the residence.

56. Beginning in or around July 2021, and continuing through March 2022, agents received geolocation data for **TT3** (GONZALEZ) pursuant to federal "ping" warrants. In reviewing geolocation data on **TT3**, agents determined that **TT3** was typically in the area of **Target Location 5** during the evening and night hours, confirming that **Target Location 5** is GONZALEZ's primary residence. Furthermore, after GONZALEZ made trips to Vancouver, WA, or Sacramento, CA, or even Mexico, he always returned to the area of **Target Location 5** according to geolocation data for **TT3**.

57. On March 7, 2022, geolocation information for **TT3**, revealed **TT3** was near the San Ysidro Port of Entry ("POE"). Border crossing records showed that on March 9, 2022, C. CAMPOS crossed the Otay Mesa POE in **Target Vehicle 9**. On March 11, 2022, geolocation information for **TT3** indicated **TT3** was moving north from the San Ysidro POE. At approximately 8:29 pm, surveillance units witnessed GONZALEZ arrive in **Target Vehicle 9** and an unknown female arrive in **Target Vehicle 8** at **Target Location 5** at the same time. The female stationed **Target Vehicle 8** inside the garage and Gonzalez

stationed his truck on the driveway of the residence. GONZALEZ was then seen entering the garage, and both GONZALEZ and the female were observed inside of the garage before the garage door closed. Based on the above information and totality of the investigation, I believe GONZALEZ currently resides at 1412 Thomasnell Way, Ceres, CA (Target Location 5).

Training and Experience Regarding Drug Trafficking and Drug Traffickers

58. As a result of my experience and training, I have learned that traffickers who deal in various quantities of controlled substances, or those that assist in that venture, maintain and tend to retain accounts or records of those transactions. Such records detail amounts outstanding, owed, or expended, along with records tending to indicate the identity of co-conspirators. These records may be kept on paper or contained in memory calculators or computers. It is also my experience that these traffickers tend to keep these accounts and records in their residence and in the areas under their control. It is my training and experience, that in the case of drug dealers, evidence is likely to be found where the dealers live. United States v. Angulo-Lopez, 791 F.2d 1394, 1399 (9th Cir. 1986). It is also my training and experience that where criminal activity is long-term or ongoing, equipment and records of the crime will be kept for some period of time. United States v. Greany, 929 F.2d 523, 525 (9th Cir. 1991).

59. Based upon my experience and training, I have learned that drug traffickers often place their assets in names other than their own to avoid detection of those assets by law enforcement and the Internal Revenue Service (IRS); that those persons are commonly family members, friends, and associates who accept title of assets to avoid discovery and detection; that traffickers also often place assets in the ownership of corporate entities to

avoid detection by law enforcement agencies and although these assets are in other individual(s) or corporate names, the traffickers continue to use these assets and exercise dominion and control over them. Typically, drug traffickers keep records of those registrations and transactions in their residence.

60. I have learned that large-scale drug traffickers often have on hand large amounts of United States currency in order to maintain and finance their ongoing business. It has been my experience that drug traffickers often keep large sums of currency, caches of drugs, financial instruments, precious metals, jewelry, automobiles and other items of value and/or proceeds of drug transactions, including evidence of financial transactions related to obtaining, transferring, secreting or spending large sums of money acquired from engaging in the acquisition and distribution of controlled substances in their residence or in the areas under their control.

61. In my experience, traffickers commonly have in their possession, that is, on their person, at their residence and in the areas under their control, firearms, including but not limited to handguns, pistols, revolvers, rifles, shotguns, machine guns and other weapons. Such firearms are used by drug violators to protect their illicit drug trafficking operations, and themselves against law enforcement and other drug violators because the illicit drug trade is an inherently dangerous illegal activity involving large amounts of valuable contraband and drug proceeds. Such property may include, but is not limited to, narcotics and other dangerous drugs, jewelry, narcotic paraphernalia, books, records, ledgers and quantities of currency.

62. In my experience, traffickers commonly have in their possession, that is on their person, at their residences, and their vehicles, and in the areas under their control and

which they have free and ready access to, drugs, including but not limited to in this case, cocaine, which they intend to distribute. It is my experience that drug traffickers commonly utilize these areas (vehicles, residences, properties, etc.) as locations to conceal their narcotics from law enforcement.

63. In my experience, drug traffickers may take or cause to be taken, photographs or videotapes of themselves, their associates, their property, and their product. Such traffickers often maintain photographs and/or videotapes at their residence or in the areas under their control.

64. In my experience, large scale traffickers often maintain in their possession and at their residence fictitious identification, including but not limited to, driver's licenses, employment cards, insurance cards, social security cards, certificates of birth and passports which are obtained by the traffickers and utilized in an effort to prevent law enforcement identification of the traffickers and their drug trafficking activities.

65. From my training and experience, I know that individuals involved in drug trafficking frequently store their drugs, drug proceeds, weapons, and other contraband in rooms and areas of their residences that appear to belong to, are controlled by, and/or are accessible to other occupants, including for example, bedrooms belonging to children, other family members, or roommates, in an effort to conceal the evidence from law enforcement and to disguise their ownership and control of the contraband in the event that it is seized. This warrant therefore seeks permission to search the entire premises of the residence for which the warrant is sought, including any location where there is reasonable cause to believe the items listed in Attachment B may be found. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 556 (1978) ("The critical element in a reasonable search is not that the owner of the

property is suspected of crime but that there is reasonable cause to believe that the specific ‘things’ to be searched for and seized are located on the property to which entry is sought.”); *United States v. Ross*, 456 U.S. 798, 820–21 (1982) (“A lawful search of fixed premises generally extends to the entire area in which the object of the search may be found and is not limited by the possibility that separate acts of entry or opening may be required to complete the search. Thus, a warrant that authorizes an officer to search a home for illegal weapons also provides authority to open closets, chests, drawers, and containers in which the weapon might be found.”); *see also United States v. Adjani*, 452 F.3d 1140, 1146 (9th Cir. 2006) (“Although individuals undoubtedly have a high expectation of privacy in the files stored on their personal computers, we have never held that agents may establish probable cause to search only those items owned or possessed by the criminal suspect. The law is to the contrary.”) (citing *Zurcher*); *United States v. Tehfe*, 722 F.2d 1114, 1118 (3d Cir. 1983) (“Property owned by a person absolutely innocent of any wrongdoing may nevertheless be searched under a valid warrant.”) (cited with approval in *Adjani*).

66. In my experience, drug traffickers often utilize vehicles in which to transport and distribute controlled substances in facilitation of their trafficking activities. It has also been my experience that traffickers will also utilize vehicles as locations in which to store controlled substances prior to distribution. During prior investigations, I have observed that drug traffickers will often utilize vehicles registered in the names of individuals other than themselves in an effort to avoid detection by law enforcement.

67. In addition, these traffickers tend to attempt to legitimize their assets by establishing domestic and foreign businesses, by creating shell corporations, by utilizing bank haven

countries and attorneys specializing in drafting and establishing such entities employed to “launder” the proceeds derived from the distribution of controlled substances.

68. In establishing these entities, the traffickers sometimes must travel to meetings in foreign countries as well as domestically. As a result of that travel, records are generated reflecting travel by commercial and private aircraft, Commercial Ocean and private vessels as well as common carrier(s).

69. Individuals involved in the distribution of cocaine and other illegal drugs often make, or cause to be made, pictures, videos, movies, compact discs, floppy discs, or other such items which are or contain photographic or digital images in order to memorialize their narcotics distribution, use, possession, or any other activities surrounding their cocaine and other drug trafficking activities, and that such items often identify co-conspirators in their drug trafficking activities.

70. It has been my experience in the past, and particularly in this case, that when suspects utilize mobile telephones to communicate with cooperating individuals or undercover agents to set up drug deals, records relating to these activities will be found stored in the cellular telephone.

71. I know that narcotics traffickers use mobile telephones to communicate with one another, either by voice or text message. Mobile telephones preserve in their memory a history of incoming, outgoing, and missed calls, which can lead to evidence of the telephone numbers of other narcotics traffickers and the dates and times that they and/or the mobile telephone user dialed one another’s telephones. Mobile telephones also contain in their memory a telephone book. This allows the user to store telephone numbers and other contact information; the information stored in a telephone used by a narcotics

trafficker is evidence of the associations of the narcotics trafficker, some of which are related to his or her illegal business. Mobile telephones also contain in their memory text messages sent, received, and drafted by the mobile telephone user. The text message history of a narcotics trafficker's mobile telephone can contain evidence of narcotics trafficking because it shows the communications or planned communications of a narcotics trafficker and the telephone numbers of those with whom the narcotics trafficker communicated or intended to communicate. Mobile telephones also have a voicemail function that allows callers to leave messages when the telephone user does not answer. Narcotics traffickers sometimes leave voice messages for each other and this is evidence both of their mutual association and possibly their joint criminal activity. Mobile telephones can also contain other user-entered data files such as "to-do" lists, which can provide evidence of crime when used by a narcotics trafficker. Mobile telephones can also contain photographic data files, which can be evidence of criminal activity when the user was a narcotics trafficker who took pictures of evidence of crime. Mobile telephone companies also store the data described in this paragraph on their own servers and associate the data with particular users' mobile telephones.

72. From my training and experience, I know that individuals that drug traffickers also frequently use computers and other electronic media to conduct their trade and to keep track of drug inventories, proceeds, and debts. This information can be found in electronic records that might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

73. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, the purpose of their use, who used them, and when.

74. Thus, the forensic analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment.

75. In cases of this sort, laptop computers and/or smartphones are also used as instrumentalities of the crime to commit offenses involving interstate drug sales and movement of drug proceeds. Devices such as modems and routers can contain information about dates, frequency, and computer(s) used to access the Internet. The laptop or smart phone may also have fingerprints on them indicating the user of the computer and its components.

76. Similarly, files related to the purchasing and selling of controlled substances, as well as the movement of currency found on computers and other digital communications devices are usually obtained from the Internet or the cellular data networks using application software which often leaves files, logs or file remnants which would tend to show the identity of the person engaging in the conduct as well as the method of location or creation

of the data, search terms used, exchange, transfer, distribution, possession or origin of the files. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary internet directory or “cache”. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed internet pages or if a user takes steps to delete them. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

77. “User attribution” evidence can also be found on a computer and is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time. Your affiant knows from training and experience that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of internet connection at the residence.

78. Searching the computer(s) for the evidence described in the attachment may require a range of data analysis techniques. For example, information regarding user attribution or internet use is located in various operating system log files that are not easily located or reviewed. In addition, a person engaged in criminal activity will attempt to conceal

evidence of the activity by “hiding” files or giving them deceptive names. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this location (the computer) for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

79. Based upon knowledge, training and experience, your affiant knows that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

- a) The nature of evidence: As noted above, not all evidence takes the form of documents and files that can be easily viewed on-site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires

considerable time, and taking that much time on premises could be unreasonable.

Also, because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a “booby-trap”), the controlled environment of a laboratory is essential to its complete and accurate analysis.

b) The volume of evidence and time required for an examination: Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Reviewing information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

c) Technical requirements: Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the

storage media off- site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d) Variety of forms of electronic media: Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

80. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to, computer-assisted scans of the entire medium that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

81. The terms “evidence” and “documents” as used above include all of the items of evidence more fully described in Attachment B in whatever form and by whatever means such evidence or documents, their drafts, or their modifications may have been created or stored.

82. As described above and in Attachments A-1 through A-17 and B, this Affidavit seeks permission to search and seize things that are related to the cocaine trafficking conspiracy between CHAVEZ, PONCE, GONZALEZ, and their co-conspirators and associates, in whatever form such things are stored. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Even when a user deletes information from a device, it can sometimes be recovered with forensics tools.

Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

83. It is my opinion, based on my training and experience, and the training and experience of other law enforcement investigators to whom I have spoken, that the items listed in Attachment B are items most often associated with the distribution of controlled substances, including cocaine, as well as the proceeds from such illegal operations.

84. Based on my experience and training, and after consulting with other law enforcement officers experienced in drug investigations, I know that individuals involved in drug dealing often maintain at their residences, vehicles, and their persons the items described in Attachment B. Individuals involved in drug dealing also often maintain paraphernalia for packaging, weighing, cutting, testing, distributing, and identifying controlled substances. Therefore, I am requesting authority to seize all the items listed in Attachment B to this Affidavit and incorporated here by reference.

85. Individuals involved in illicit activities that generate large amounts of income will conduct cash purchases, the purchasing of numerous monetary instruments with cash in amounts less than \$10,000 to avoid reporting requirements, the use of aliases and nominees, the use of businesses as “fronts” in an attempt to legitimize and conceal activities, the use of wire remitter companies to convert into wire transfers below reporting requirements and the use of “off-shore” banking in an attempt to break the paper trail. These and other schemes are commonly referred to as “money laundering.”

86. Individuals involved in illicit activities normally maintain records of their financial activity, such as receipts for expenditures by cash and check, bank records, and other financial documents, in their personal residences and place of business. Furthermore,

individuals engaged in an income-producing business keep records of the financial activities of the business for numerous reasons and often use accountants to complete financial statements and tax returns for their business and personal tax returns.

87. Individuals involved in illicit activities maintain evidence of their crimes for long periods of time. The evidence may be necessary business records that must be kept for information reporting purposes, such as for state and Federal tax returns, and loan applications. The evidence may also be innocuous at first glance (e.g., financial, credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, check books, videotapes and photographs, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone and pager bills, keys to safe deposit boxes, packaging materials, computer hardware and software), but have significance and relevance when considered in light of other evidence. The criminal offender may no longer realize he/she still possesses the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. The criminal offender may also be under the mistaken belief that he/she has deleted, hidden or further destroyed any computer-related evidence that may be retrievable by a trained forensic computer expert.

88. Individuals who amass proceeds from both legal and illegal activities routinely attempt to further that conduct, and/or in the case of illegal activities conceal the existence and source of their funds, by engaging in financial transactions with domestic and foreign institutions, and others, through all manner of financial instruments, including cash, cashier's checks, money drafts, traveler's checks, wire transfers, money orders, etc.

Records of such instruments are routinely maintained at the individual's residence or place of business.

89. The net worth/source and application of funds analysis show that a person's known expenditures and/or accumulation of assets substantially exceed their legitimate source of income to prove that the suspect is engaged in either legal or illegal money generating activities, such as real estate investing or narcotics trafficking. The net worth analysis compares a suspect's net worth (cost value of total assets minus total liabilities) at a time just before the suspect has commenced his/her purported criminal enterprise, to his/her net worth at the approximate time of his/her cessation of criminal activity.

90. The source and application of the funds analysis focuses on the suspect's expenditures during the time period of the purported illegal activities and compares such expenditures with his/her legitimate source of income. Both analysis require evaluation of bank records, credit records, loan records, documents evidencing ownership of assets, and other documents evidencing the financial profile of the suspect during the course of the purported illegal activity, as well as a short time period prior to the illegal activity (e.g., one year).

Other than assisting in the net worth/source and application of funds analysis, a financial profile of a suspect prior to the purported criminal activity that are consistent with a person generating income from illegal activities (e.g., drug or firearms trafficking), as compared to a person earning income from legitimate sources. Evidence of a defendant's expenditures, asset accumulation, financial life-style, net worth/source and application of funds analyses, and underlying financial documents necessary for such analysis are admissible evidence under federal case law. Thus, there is a bona fide reason for the need for such documents to be taken during the execution of a search warrant.

91. Individuals involved in drug trafficking often maintain, on hand, large amounts of U.S. currency in order to maintain and finance their ongoing drug business. These individuals conceal caches of drugs, large amounts of currency, financial instruments, precious metals, jewelry, and other items of value and/or proceeds of drug transactions, and evidence of financial transactions relating to obtaining, transferring, secreting, or spending of large sums of money made from engaging in drug trafficking activities, in their residences, offices, garages, automobiles, storage buildings, and safety deposit boxes.

92. **REQUEST FOR SEALING:** I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

[CONTINUED ON NEXT PAGE]

Conclusion

93. The facts in this Affidavit demonstrate probable cause to believe that Jose CHAVEZ, Denis PONCE, and Mario GONZALEZ, and other co-conspirators and associates are involved in the above-described offenses, and that evidence, fruits, and instrumentalities of these offenses, as described in Attachment B, are likely to be found at the locations and in the vehicles listed in Attachments A-1 through A-17.

I swear under penalty of perjury, that the foregoing information is true and correct to the best of my knowledge, information and belief.

Orcina A. Pacheco-Garcia
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed to me telephonically on March __, 2022.

Hon. Deborah Barnes
United States Magistrate Judge

Approved as to form:

/s/ David Spencer
David W. Spencer
Assistant United States Attorney

Attachment A-1

DESCRIPTION OF LOCATION TO BE SEARCHED



The property to be searched is 3505 Condor Ct, Carmichael, CA 95608 and is pictured above and identified as follows: A one-story residence with brown coloring and a partial brick exterior. There is a garage located at the front of the house. The premises to be searched includes all rooms, attics, basements, and other parts therein, the surrounding grounds and any garages, storage rooms, or outbuildings of any kind located thereon to which the occupants of 3505 Condor Ct, Carmichael, CA 95608 have access.

Attachment A-2

DESCRIPTION OF LOCATION TO BE SEARCHED



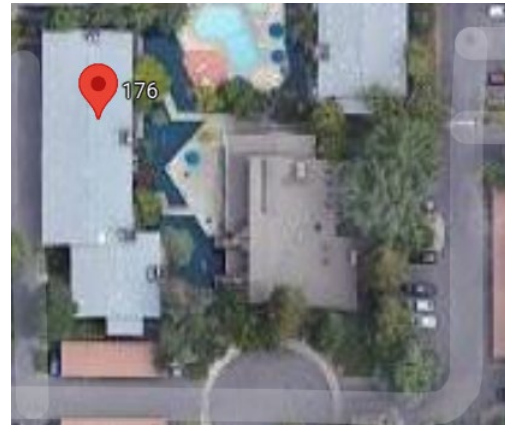
The property to be searched is 2533 Del Paso Boulevard, Sacramento, California, and is pictured above and identified as follows: A two-story business, the building has a “LA VICTORIA” sign with red letters in the front. There are two connected glass metal front doors. The premises to be searched includes all office rooms, compartments, and storage rooms or areas, including basements and/or attics and safes that are located thereon.

Attachment A-3
DESCRIPTION OF LOCATION TO BE SEARCHED



The property to be searched is 2556 Rio Linda Boulevard, Sacramento, California, and is pictured above and identified as follows: A one-story residence with brown coloring. There is a black iron gate surrounding the entire property with a back alley to Del Paso Rio Linda Blvd. Various large vehicles are parked inside of the locked gate of the residence. The premises to be searched includes all rooms, attics, basements, and other parts therein, the surrounding grounds and any garages, vehicles parked inside of the premises, storage rooms, or outbuildings of any kind located thereon to which the occupants of 2556 Rio Linda Boulevard, Sacramento, California have access.

Attachment A-4
DESCRIPTION OF LOCATION TO BE SEARCHED



The property to be searched is 2480 Larkspur Lane, #176, Sacramento, California, and is pictured above and identified as follows: A one-story condominium with brown coloring. Condo #176 is located on the left side of the second floor. There is a wooden sign on the stairway with 176 and 175 for two upstairs condos. The premises to be searched includes all rooms, attics, basements, and other parts therein, the surrounding grounds and any garages, storage rooms, or outbuildings of any kind located thereon two which the occupants 2480 Larkspur Lane, #176, Sacramento, California have access.

Attachment A-5
DESCRIPTION OF LOCATION TO BE SEARCHED



The property to be searched is 1412 Thomasnell Way, Ceres, California, and is pictured above and identified as follows: A one-story residence with brown coloring. There are two garage doors at the front of the house. The numerals 1412 are located in the front of the home. The premises to be searched includes all rooms, attics, basements, and other parts therein, the surrounding grounds and any garages, storage rooms, or outbuildings of any kind located thereon to which the occupants 1412 Thomasnell Way, Ceres, California have access.

Attachment A-6

TARGET VEHICLE 1 – 2018 Volkswagen sedan, white with license plate **8HKN876**, registered to Jose CHAVEZ at 3505 Condor Court, Carmichael, CA.

B. The search of TARGET VEHICLE 1 is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities.

Attachment A-7

TARGET VEHICLE 2 –2016 Honda, grey with license plate **8MHH330**, registered to Jose M CHAVEZ at 3505 Condor Court, Carmichael, CA.

B. The search of TARGET VEHICLE 2 is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities.

Attachment A-8

TARGET VEHICLE 3 –2020 Honda SUV, black with license plate **8NKA590**, registered to Jose M CHAVEZ at 3505 Condor Court, Carmichael, CA.

B. The search of TARGET VEHICLE 3 is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities.

Attachment A-9

TARGET VEHICLE 4- 2017 Honda Silver, silver with license plate **8KIV189**, registered to Jose M CHAVEZ at 3505 Condor Court, Carmichael, CA.

B. The search of TARGET VEHICLE 4 is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities.

Attachment A-10

TARGET VEHICLE 5- 2017 Honda Silver, silver with license plate **7UWH104**, registered to Denis Castillo, at 7987 Old Winding Way, Fair Oaks, CA.

B. The search of TARGET VEHICLE 5 is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities.

Attachment A-11

TARGET VEHICLE 6- 2007 Saturn grey, with license plate 6WCJ577 registered to Denis Ponce Castillo, at 3825 Presidio St, Sacramento, CA.

B. The search of TARGET VEHICLE 6 is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities.

Attachment A-12

TARGET VEHICLE 7- 2008 Toyota Tacoma with license plate 81749E3, registered to Denis Ponce, at 3825 Presidio St, Sacramento, CA.

B. The search of TARGET VEHICLE 7 is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities.

Attachment A-13

TARGET VEHICLE 8- 2021 Toyota Camry, white with license plate **8UHG728**, registered to Mario Naranjo, at 1412 Thomasnell Way, Ceres, CA.

B. The search of TARGET VEHICLE 8 is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities.

Attachment A-14

TARGET VEHICLE 9 – 2017 GMC, red truck, CA license # 98560C2, registered to Jose CHAVEZ, at 3505 Condor Court, Carmichael, CA.

B. The search of TARGET VEHICLE 9 is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities.

Attachment A-15

TARGET VEHICLE 10 - 2007 Toyota, silver Tacoma, CA license # 36821B3, registered to Jose CHAVEZ, at 3505 Condor Court, Carmichael, CA.

B. The search of TARGET VEHICLE 10 is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities.

Attachment A-16

TARGET VEHICLE 11- 1994 Jaguar, CA license plate **3KST304**, registered to Jose M CHAVEZ at 3505 Condor Court, Carmichael, CA.

B. The search of TARGET VEHICLE 11 is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities.

Attachment A-17

TARGET VEHICLE 12- 1998 Ford truck CA license plate **8V96908**, registered to Jose M CHAVEZ at 2533 Del Paso Blvd., Sacramento, CA.

B. The search of TARGET VEHICLE 12 is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities.

Attachment B
Items to be Seized

Law enforcement is authorized to search and seize property that constitutes evidence, fruits, and instrumentalities of violations of the following federal statutes (the “Target Offenses”):

- 21 U.S.C. §§ 841(a)(1) and 846 – Conspiracy to distribute and possess with intent to distribute cocaine.
- 21 U.S.C. § 841(a)(1) – Distribution and possession with intent to distribute cocaine.

As further described in the Affidavit, the specific evidence, fruits, and instrumentalities of the Target Offenses for which agents may search includes:

1. Controlled substances, including cocaine or items used to distribute controlled substances; drug-trafficking paraphernalia, including scales, measuring devices, and weighing devices; narcotics diluting or cutting agents; narcotics packaging materials, including plastic, tin foil, cellophane, jars, plastic bags, and containers; and plastic surgical gloves;
2. United States and foreign currency linked to drug trafficking and/or the proceeds of drug trafficking, including the pre-recorded U.S. currency used to purchase cocaine during this investigation;
3. Narcotics or money ledgers, narcotics distribution or customer lists, narcotics supplier lists, correspondence, notations, logs, receipts, journals, books, pay and owe sheets, records and other documents noting the price, quantity, date and/or times when narcotics were purchased, possessed, transferred, distributed, sold or concealed;
4. Telephone paging devices, beepers, mobile phones, car phones, answering machines and tapes, and other communication devices which could be used to participate in a conspiracy to distribute controlled substances in violation of 21 U.S.C. § 841(a)(1);
5. Bank account records, wire transfer records, bank statements, safety deposit keys and records, money wrappers, money containers, income tax returns, evidence of financial transfer, or movement of money generated from the sale of narcotics;
6. Personal telephone books, address books and other such address listings, letters, cables, telegrams, telephone bills, photographs, audio and video tapes connected to drug trafficking, personal notes and other items reflecting names, addresses, telephone numbers, communications, and illegal activities of associates in drug trafficking activities;
7. Financial instruments purchased with large amounts of currency derived from the sale of controlled substances, including traveler’s checks, bonds, stock certificates, cashier’s checks and

certificates of deposit; money counting machines, money wrappers and bags used to carry controlled substances;

8. Records, documents and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry, or other items obtained with the proceeds from the sale of controlled substances;

9. Records, items, and documents reflecting travel, including airline tickets, credit card receipts, travel vouchers, hotel and restaurant receipts, canceled checks, maps and written directions to location;

10. Handguns, shotguns, rifles, explosives, and other firearms/incendiary devices and ammunition that may be used to facilitate the distribution or possession of, with the intent to distribute controlled substances or discovered in the possession of a prohibited person; and

11. Indicia of occupancy, residency, control or ownership of the premises and things described in this warrant, including utility bills, telephone bills, loan payment receipts, rent documents, canceled envelopes and keys, photographs, and bank records.

12. Any digital devices or other electronic storage media and/or their components used as a means to commit the violations described above, including:

a. any digital device or other electronic storage media capable of being used to commit, further, or store evidence or fruits of the Target Offenses;

b. any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

c. any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. any passwords, password files, seed words, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

13. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. Any and all names, words, telephone numbers, email addresses, time/date information, messages or other electronic data in the memory of these digital devices or other electronic storage media or on a server and associated with these digital devices or other electronic storage media, including:

- i. Incoming call history;
- ii. Outgoing call history;
- iii. Missed call history;
- iv. Outgoing text messages;
- v. Incoming text messages;
- vi. Draft text messages;
- vii. Telephone book;
- viii. Emails;
- ix. Data screen or file identifying the telephone number associated with the mobile telephone searched;
- x. Data screen, file, or writing containing serial numbers or other information to identify the electronic device searched;
- xi. Voicemail;
- xii. User-entered messages (such as to-do lists); and
- xiii. Stored media such as photographs or video.

b. Any and all locations, addresses, GPS coordinates, names, time/date information, or other electronic data related to addresses and driving directions.

c. All information and records related to violations of 21 U.S.C. § 841(a) (drug trafficking) and/or 21 U.S.C. § 846 (conspiracy to traffic drugs), including but not limited to:

- i. Data and information related to stored applications and/or websites used to communicate with associates and co-conspirators;
- ii. Data, information, or documents related to the manufacture of controlled substances, including the acquisition, possession, and use of equipment, paraphernalia, chemicals, and materials used in the manufacturing process;
- iii. lists of customers and related identifying information;
- iv. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- v. any information related to sources of drugs or drug manufacturing materials and equipment (including names, addresses, phone numbers, email addresses, or any other identifying information);

- vi. any information recording schedule or travel;
- vii. all bank records, checks, credit card bills, account information, and other financial records;
- viii. data, information, or documents related to the receipt of proceeds from controlled substances distribution and the transfer, investment, control, and disposition of those proceeds;
- ix. records of Internet Protocol addresses used;
- x. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- xi. any communications related to drug trafficking;
- xii. stored media such as photographs or video.

d. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

e. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

f. evidence of the lack of such malicious software;

g. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

i. evidence of the times the digital device or other electronic storage media was used;

j. passwords, encryption keys, seed words, and other access devices that may be necessary to access the digital device or other electronic storage media;

k. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

l. contextual information necessary to understand the evidence described in this attachment.

14. Records and things evidencing the use of an Internet Protocol (IP) address to communicate with the internet, including:

- a. routers, modems, and network equipment used to connect computers to the internet;
- b. records of Internet Protocol addresses used;
- c. records of internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIME.

United States v. Chavez, et al.
Penalties for Criminal Complaint

Defendants

Jose Manuel CHAVEZ Zepeda
Denis Zacarias PONCE Castillo

COUNT 1: **ALL DEFENDANTS**

VIOLATION: 21 U.S.C. §§ 846, 841(a)(1) - Conspiracy to Distribute and Possess with Intent to Distribute at least 500 grams of a Mixture and Substance containing Cocaine

PENALTIES: Mandatory minimum of 5 years in prison and a maximum of up to 40 years in prison; or
Fine of up to \$5,000,000; or both fine and imprisonment
Supervised release of at least 4 years up to life

SPECIAL ASSESSMENT: \$100 (mandatory on each count)

COUNT 2: **ALL DEFENDANTS**

VIOLATION: 21 U.S.C. § 841(a)(1) – Distribution of at least 500 grams of a Mixture and Substance containing Cocaine

PENALTIES: Mandatory minimum of 5 years in prison and a maximum of up to 40 years in prison; or
Fine of up to \$5,000,000; or both fine and imprisonment
Supervised release of at least 4 years up to life

SPECIAL ASSESSMENT: \$100 (mandatory on each count)

ORIGINAL

FILED IN OPEN COURT
U.S.D.C. - Atlanta

JUN 13 2017

By: JAMES N. HATTEN, Clerk
Cem Deputy Clerk

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA

v.

OSCAR PEREZ (AKA OSCAR
GUSTAVO PEREZ-BERNAL);
ITZAYANA PEREZ (AKA
ITZAYANA GUADALUPE PEREZ-
BERNAL, "LUPE")

UNDER SEAL

Criminal Indictment

No. **1:17 CR200**

THE GRAND JURY CHARGES THAT:

Count One

Money Laundering Conspiracy
(18 U.S.C. § 1956(h))

1. Beginning in or about 2013, and continuing to on or about the date of this Indictment, the exact dates unknown to the Grand Jury, in the Northern District of Georgia and elsewhere, the defendants, OSCAR PEREZ (aka OSCAR GUSTAVO PEREZ-BERNAL) and ITZAYANA PEREZ (aka ITZAYANA GUADALUPE PEREZ-BERNAL, "LUPE"), did knowingly combine, conspire, and agree with each other and with others, both known and unknown to the Grand Jury, to commit offenses against the United States in violation of Title 18, United States Code, Section 1956 to wit:

- a) to knowingly conduct and attempt to conduct financial transactions affecting interstate commerce and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, proceeds from

the sale and distribution of a controlled substance, knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i); and

- b) with the intent to conceal and disguise the nature, location, source, ownership and control, of property believed to be the proceeds of specified unlawful activity, to knowingly conduct and attempt to conduct a financial transaction affecting interstate or foreign commerce involving property represented to be proceeds of specified unlawful activity, that is proceeds from the sale and distribution of a controlled substance, by a law enforcement officer and by another person at the direction of, and with the authorization of, a federal official authorized to investigate and prosecute violations of this section, in violation of Title 18, United States Code, Section 1956(a)(3)(B).

Background

2. During the above-listed time period, OSCAR PEREZ (hereinafter "PEREZ"), operated a convenience store named "La Tienda" and a small restaurant named "Cocina Linda Vista," both of which were located in

Chamblee, Georgia. PEREZ's sister, ITZAYANA PEREZ (hereinafter "ITZAYANA"), also worked at La Tienda.

3. La Tienda and Cocina Linda Vista offered various services to their customers, including the ability to electronically transmit funds to other countries (commonly referred to as "remittances"). In order to transmit customers' funds internationally, both stores entered into agency agreements with various "money transmitters." These money transmitters specialized in electronically wiring money and had agent locations throughout the United States and other countries. In practice, individuals seeking to use one of these money transmitters brought currency to an agent location (oftentimes, a convenience store or grocery store). The agent collected the funds along with certain information from the customer, such as the recipient's name and contact information, and provided the customer with a verification code that the recipient could use to retrieve the funds from another agent location. The money transmitters therefore provided a means for customers to securely and rapidly transmit funds throughout the world. During the above-listed time period, PEREZ and ITZYANA wired funds internationally using the money transmitters' electronic wiring systems.

4. The money transmitters charged customers a fee for using their services. The money generated from this fee was split between the agent that processed the customer's transaction and the money transmitter. Each of the money transmitters prohibited its agents, including La Tienda and Cocina Linda Vista,

from charging customers additional fees or commissions for transmitting customers' funds.

5. The money transmitters were each registered with the U.S. Department of Treasury, Financial Crimes Enforcement Network ("FinCEN"), which permitted them to wire third party funds. During the above-listed time period, the Bank Secrecy Act (31 U.S.C. § 5300, *et. seq.*) and its implementing regulations imposed certain recordkeeping and reporting requirements upon money transmitters and their agents.

6. For example, the Bank Secrecy Act and its implementing regulations required these money transmitters to file certain reports with FinCEN regarding financial transactions that involved suspicious or potentially illegal activity. 31 U.S.C. § 5318(g)(1); 31 C.F.R. § 1022.320(a)(2). These reports were commonly known as "Suspicious Activity Reports" (SARs). Pursuant to 31 C.F.R. § 1022.320(a)(2), the money transmitter was required to file a SAR if the financial transaction at issue involved at least \$2,000 in funds and the business knew, suspected, or had reason to suspect that the transaction (or a pattern of transactions of which the transaction was a part):

- a. involved funds derived from illegal activity or was intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any Federal law

- or regulation or to avoid any transaction reporting requirement under Federal law or regulation;
- b. was designed, whether through structuring or other means, to evade any requirements of this chapter or of any other regulations promulgated under the Bank Secrecy Act;
- c. served no business or apparent lawful purpose, and the reporting money services business knew of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or
- d. involved use of the money services business to facilitate criminal activity.

7. Money transmitters were also required to maintain records related to certain high dollar transfers; for each transmission of \$3,000 or more, money transmitters were required to record the sender's name and address. 31 C.F.R. § 1010.410(e). At least some of the above-listed money transmitters imposed additional requirements upon their agents. For instance, on November 22, 2013, PEREZ certified his understanding that one particular money transmitter required its agents to obtain identification from customers seeking to transmit more than \$2,000 per day.

8. The money transmitters required their agents to comply with the Bank Secrecy Act. During at least part of the conspiracy, PEREZ served as the Bank

Secrecy Act / Anti-Money Laundering Compliance Officer for La Tienda and Cocina Linda Vista. On November 22, 2013, PEREZ signed an "Agent's Ethical Code of Conduct Acknowledgement" on behalf of La Tienda in which he agreed that he would not, among other things: recommend that customers split wires by using fictitious names to send multiple wire transfers; allow customers to wire money if he had knowledge or suspected that the funds were potentially the proceeds from illegal activity; accept or solicit bribes, tips or gifts to facilitate money laundering for customers; or permit customers to use false identification to wire money.

9. To further comply with the Bank Secrecy Act, the money transmitters mandated that agents undergo periodic training. On a September 2, 2015, anti-money laundering compliance test, PEREZ defined money laundering as "hiding the origin of money using a process of placement, process and integration" and answered that when encountering suspicious activity, he should report the activity to the money transmitter's compliance department.

10. During the above-listed time period, PEREZ and ITZAYANA along with other individuals known and unknown to the Grand Jury, used La Tienda and Cocina Linda Vista to transmit over \$16.9 million through the money transmitters' electronic wiring systems. The vast majority of these wires were directed to recipients in different countries, including, most typically, Mexico.

Manner and Means

11. During the time period of the conspiracy, PEREZ and ITZAYANA accepted kickbacks from customers who sought to transmit drug proceeds out of the country. These kickbacks exceeded the set fees charged by the money transmitters and were in direct violation of the money transmitters' agreements with La Tienda and Cocina Linda Vista.

12. PEREZ and ITZAYANA helped their customers hide the source of the funds by listing false sender names, addresses, and telephone numbers on the wires. PEREZ and ITZAYANA also intentionally "split" the wires into smaller amounts in the hopes of evading detection from the money transmitters' internal compliance programs.

13. PEREZ and ITZAYANA transferred money to Mexico for cooperating law enforcement sources as well as an undercover law enforcement officer who all stated that the funds came from the sale of narcotics. In exchange for kickbacks that exceeded the fees authorized by the money transmitters, PEREZ and ITZAYANA concealed the nature, origin, and source of these funds by listing fake names, addresses, and telephone numbers as the true senders and agreeing to split the wires into smaller amounts.

14. On or about April 27, 2015, ITZAYANA transferred funds on behalf of "Cooperating Source One" in exchange for a kickback that exceeded the fees authorized by the money transmitters. During the course of an exchange at La Tienda, ITZAYANA told Cooperating Source One that people moving money

typically let PEREZ know ahead of time that they are coming and that she and PEREZ did not send the wires all at the same time so that the money transmitters believed multiple people were coming in and out of the store. Cooperating Source One claimed to be a middle person who worked for someone that sold drugs. ITZAYANA conducted multiple wire transfers to Mexico for Cooperating Source One that listed fake sender names, addresses, and telephone numbers.

15. On or about November 4, 2015, PEREZ transferred funds to Mexico for Cooperating Source Two in exchange for a kickback that exceeded the fees already charged by the money transmitter. During the course of an exchange with PEREZ at La Tienda, Cooperating Source Two claimed a need to find a way to transmit \$100,000, which the source had obtained from people who were sending "merchandise." PEREZ told the cooperating source that he wanted to help but that he also transmitted money for others. PEREZ suggested that he could stagger the transactions by transmitting \$20,000 a day for the cooperating source. The cooperating source indicated that this might work and that the people the cooperating source was working with would then be able to send the "merchandise." PEREZ conducted multiple transfers to Mexico for the cooperating source that listed fake sender names, addresses, and telephone numbers.

16. On or about April 25, 2017, PEREZ met with Cooperating Source Two at La Tienda. During the meeting, Cooperating Source Two told PEREZ that the

money she had previously brought came from selling “frio,” a common name for methamphetamine. Cooperating Source Two claimed to have \$100,000 from selling “coke,” a common name for cocaine, that the source wanted Perez’s help in moving to Mexico. PEREZ agreed to transmit these funds in exchange for a kickback of \$20 per wire. However, Cooperating Source Two did not return to La Tienda.

All in violation of Title 18, United States Code, Section 1956(h).

Count Two
Sting Money Laundering
 (18 U.S.C. §§ 1956(a)(3)(B) and 2)

17. The Grand Jury re-alleges and incorporates by reference the factual allegations contained in paragraphs 1 through 16 of this Indictment as if fully set forth herein.

18. On or about April 27, 2015, in the Northern District of Georgia, the defendant, ITZAYANA PEREZ, aided and abetted by others known and unknown to the Grand Jury, with the intent to conceal and disguise the nature, location, source, ownership and control of property believed to be the proceeds of specified unlawful activity, did knowingly conduct and attempt to conduct a financial transaction affecting interstate or foreign commerce involving property represented to be proceeds of specified unlawful activity, that is, proceeds from the sale and distribution of a controlled substance, by a person at the direction of,

and with the authorization of, a federal official authorized to investigate and prosecute violations of this section.

All in violation of Title 18, United States Code, Sections 1956(a)(3)(B) and 2.

Count Three

Sting Money Laundering

(18 U.S.C. §§ 1956(a)(3)(B) and 2)

19. The Grand Jury re-alleges and incorporates by reference the factual allegations contained in paragraphs 1 through 16 of this Indictment as if fully set forth herein.

20. On or about November 4, 2015, in the Northern District of Georgia, the defendant, OSCAR PEREZ, aided and abetted by others known and unknown to the Grand Jury, with the intent to conceal and disguise the nature, location, source, ownership and control of property believed to be the proceeds of specified unlawful activity, did knowingly conduct and attempt to conduct a financial transaction affecting interstate or foreign commerce involving property represented to be proceeds of specified unlawful activity, that is, proceeds from the sale and distribution of a controlled substance, by a person at the direction of, and with the authorization of, a federal official authorized to investigate and prosecute violations of this section.

All in violation of Title 18, United States Code, Sections 1956(a)(3)(B) and 2.

Forfeiture

21. Upon conviction of one or more of the offenses alleged in Counts One through Three of the Indictment, the defendants, OSCAR PEREZ (aka OSCAR GUSTAVO PEREZ-BERNAL) and ITZAYANA PEREZ (aka ITZAYANA GUADALUPE PEREZ-BERNAL, "LUPE"), shall forfeit to the United States pursuant to Title 18, United States Code, Section 982(a)(1), any property, real or personal, involved in the money laundering offenses and all property traceable to such property including, but not limited to, a sum of money in United States currency representing the total amount of money involved in each offense for which the defendant is convicted.

22. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

- a. Cannot be located upon the exercise of due diligence;
- b. Has been transferred or sold to, or deposited with, a third party;
- c. Has been placed beyond the jurisdiction of the court;
- d. Has been substantially diminished in value; or
- e. Has been commingled with other property which cannot be divided without difficulty;

It is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b), to seek forfeiture of any other property of said defendants up to the value of the forfeitable property described above; all pursuant to Title 18, United States Code,

Sections 981(a)(1)(C) and 982(a)(2)(B), and Title 28, United States Code, Section 2461(c).

A True BILL
C
FOREPERSON

JOHN A. HORN

United States Attorney



THOMAS J. KREPP

Assistant United States Attorney

Georgia Bar No. 346781



ALISON B. PROUT

Assistant United States Attorney

Georgia Bar No. 141666

600 U.S. Courthouse

75 Ted Turner Drive SW

Atlanta, GA 30303

404-581-6000; Fax: 404-581-6181

We only use cookies that are necessary for this site to function to provide you with the best experience. The controller of this site may choose to place supplementary cookies to support additional functionality such as support analytics, and has an obligation to disclose these cookies. Learn more in our [Cookie Statement](#).



Homeland
Security

Subscribe to updates from U.S. Department
Security

Email Address e.g. name@e:

October 2024, Issue #57

U.S. Department of Homeland Security sent this bulletin at 10/11/2024 10:31 AM EDT

Share Bulletin



October 2024 | Issue #57



Money Service Businesses (MSB) are financial institutions that offer various money-related services, including currency exchange, money transfers, check cashing, and issuing or redeeming money orders. These businesses serve as an important financial link, particularly for individuals who may not have access to traditional banking services.

However, MSBs can be vulnerable to abuse, particularly to money laundering, fraud, and other financial crimes. While the majority of MSBs operate lawfully and take necessary precautions to prevent illegal activity, some may become complicit, either knowingly or unknowingly, in facilitating problematic transactions. The decentralized nature of some MSBs, combined with large cash transactions and international transfers, can make it harder for regulatory bodies to monitor suspicious activity, increasing the risk of their involvement in illicit activity.

What is a “Complicit MSB”?

A complicit MSB is an MSB that cooperates with a drug trafficking organization (DTO) to launder narcotics proceeds is complicit in the illegal activity and wrongdoing. The following is an explanation of how complicit MSB's operate:

Mexican DTO's use cities in the United States as distribution points for narcotics. Once their products have been sold, narcotics traffickers must find a way to return the proceeds from these sales to Mexico. To accomplish this goal, some Mexican DTO's partner with complicit MSB's. Complicit MSB's will accept narcotics proceeds, in the form of bulk U.S. currency, from couriers that work for Mexican DTO's. In addition to bulk U.S. currency, the courier, or another member of the DTO, will provide complicit MSB's with a list of payee names in Mexico. The complicit MSB will structure the bulk U.S. currency into smaller amounts (historically between \$500-\$999; however, increasingly in excess of \$1,000) and then send wire transfers to Mexico using the list of payee names as recipients. The complicit MSB falsifies the information for the sender of the wire transfer, to include name, address, and phone number. Once the wire transfers have been sent, the complicit MSB will text photos of the receipts from the transactions to the DTO. The receipts prove to the DTO that the transfers have been conducted and provide the information necessary for these wire transfers to be redeemed in Mexico. For their participation in the money laundering conspiracy complicit MSB's collect a fee, often 10%, of the total bulk currency provided to them.

Why are some MSBs prone to being complicit?

Several factors can increase an MSB's susceptibility to becoming complicit in financial fraud:

- **Insufficient Know Your Customer (KYC) procedures:** KYC regulations require financial institutions to verify the identity of their clients to prevent illegal activities. MSBs that neglect these procedures may inadvertently facilitate transactions for individuals involved in fraud, money laundering, or terrorism financing.
- **Poor compliance with Anti-Money Laundering (AML) regulations:** MSBs are required to report suspicious activity to FinCEN and comply with AML laws. However, some MSBs fail to invest in the necessary resources to ensure compliance, making them easier targets for criminal exploitation.
- **High volume of cash transactions:** MSBs often deal with large amounts of cash, which is more difficult to trace than electronic transactions. This can create opportunities for criminals to “clean” criminal proceeds by moving it through an MSB, knowing that the cash-based nature of the business makes it harder to detect illicit funds.
- **Limited oversight:** Some MSBs, especially smaller, independent ones, may not be subject to the same level of scrutiny as larger financial institutions, which can make it easier for criminals to exploit weaknesses in their processes.



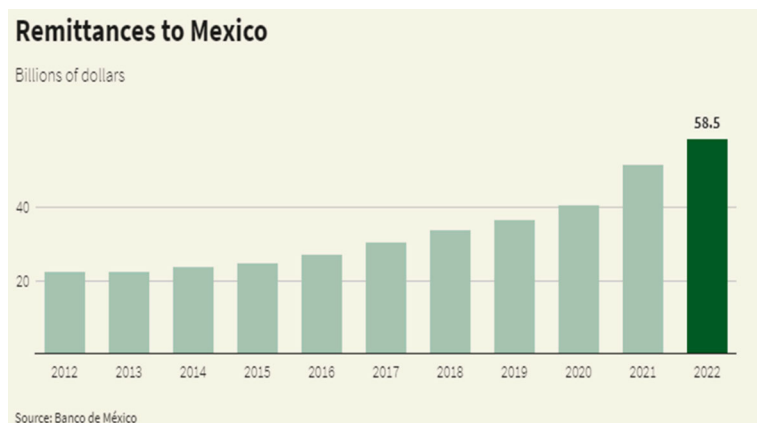
How big of a problem is this?

Remittances to Mexico, nearly all of which come from the United States, hit a record \$58.5 billion last year (2022), according to data from Mexico's central bank. That's an increase of \$25 billion, or 74%, compared to 2018, when President Andrés Manuel López Obrador came to power. Mexico's economy has been slow to recover from the coronavirus pandemic, a factor that has boosted migration to the United States in recent years along with the remittances that workers send home.

The cartels are awash in cash from U.S. sales of fentanyl, cocaine, heroin, methamphetamines and marijuana. Presently, up to 10% of all Mexico-bound remittances may be drug money moved by criminal organizations like the Sinaloa Cartel and the Jalisco New Generation Cartel. A March report by the Mexican think tank Signos Vitales estimated

new Generation Capital Market report by the Mexican bank Citigroup, estimates that at least \$4.4 billion, or 7.5%, of remittances sent to Mexico last year could come from illegal activity.

[reuters.com/investigates/special-report/mexico-drugs-remittances/](https://www.reuters.com/investigates/special-report/mexico-drugs-remittances/)



Transaction Record Analysis Center (TRAC)

Utilizing the TRAC database is important for investigators who are interested in working money laundering and narcotics investigations. For investigators that are working, or want to work, money laundering cases involving Mexican DTO's or complicit MSB agents, it is extremely important to utilize the TRAC database. Complicit MSB agents can be identified by other means but the most effective method is using the wire transfer data uploaded to TRAC.

In January 2014, as a result of a Settlement Agreement Amendment between the Arizona Attorney General and Western Union, the Transaction Record Analysis Center (TRAC) was created. The TRAC Data System has evolved into a centralized searchable database containing subpoenaed financial transactions (money transfers) from numerous global money services businesses (MSBs). Subpoenaed transactions consist of only person to person money transfers (no commercial transactions) of at least \$500 and greater primarily sent from or paid in U.S. Southwest Border States and Mexico. The Transaction Record Analysis Center is staffed by analysts and current/former law enforcement professionals recognized as experts related to money laundering activity conducted through MSBs. The TRAC Data System is exclusively available to authorized federal, state and local law enforcement while TRAC analysts provide meaningful transaction data analysis, collaboration and anti-money laundering (AML) training to TRAC users and MSB Compliance personnel in their efforts to disrupt criminal organizations and enhance anti-money laundering knowledge and techniques.

As of July 2024, TRAC has 337,158,470 transactions from 28 different MSBs, 22 of which are actively producing records. In order, the top five producers of transactions are as follows:

CES (Ria), Western Union, Intermex, BTS, Moneygram.

Red Flag Indicators



The following are some of the red flags that are indicative of a Money Service Business (MSB) that is complicit in laundering narcotics proceeds through wire transfers:

1. Heavy concentration of sent transfers paid in one primary drug source state in Mexico.

Mexican drug trafficking organizations (DTO) control narcotics distribution in various cities throughout the United States. When a complicit MSB is utilized to launder narcotics proceeds, through hundreds and thousands of wire transfers, the origin of the DTO becomes apparent through repeated use of a single payee agent state in Mexico. This becomes even more apparent when compared to other nearby MSB agent locations.

2. Complicit MSB agents will often send multiple transfers in a single day to the same drug source state in Mexico or will send several transactions in rapid succession (sometimes only minutes apart), or both (transactions conducted soon after one another and sent to the same drug source state). Law enforcement refer to these groupings as “Clusters” or “Bursts”.

“Clusters” and “Bursts” will appear in the data when a complicit MSB receives bulk currency, structures this amount into numerous smaller amounts, and then sends those amounts via wire transfer, often to the same drug source state.

3. Unique money transfer principal amounts repeated in daily activity and/or are concentrated in a dollar range.

For multiple wire transfers to be sent from the same location, for the exact same principal amount, on the same day, is highly suspicious. The chances of 11 different legitimate customers, utilizing the same MSB location, on the same day, to each send \$970, is very low. However, if an MSB is fabricating sender information to launder narcotics proceeds, the chances that they will use the same principal amount numerous times on the same day is high.

4. Lack of commonalities between the surnames of sender and receiver names.

Many individuals utilize wire transfers to send money they have earned legitimately in the United States to their family in Mexico. When this occurs, there will often be a common surname for both the sender and receiver. When a complicit MSB is fabricating the names of senders, or misappropriating the personal information of legitimate customers, common surnames between the sender and receiver will decrease.

5. Payee names receiving payments from several individuals located in several different U.S. states.

Mexican DTO's will often use a single payee name, numerous times. Since these DTO's operate cells in various U.S. states, these payees will often receive payments from more than one geographic area. For example, a payee name controlled by a Mexican DTO may receive payments from Georgia, Ohio, Colorado, and California.

6. Lack of transparency in operations/licensing:

If the MSB provides limited information about their procedures, fees, or licenses, this could indicate a lack of proper regulation or a potential for misconduct.

7. Inconsistent compliance with regulations:

An MSB that is not compliant with KYC or AML standards, or is hesitant to provide information regarding these policies, is a major red flag.

8. Unusually high rates for services:

Excessively high or unusually fluctuating rates for basic services like money transfers or currency exchange could indicate that the MSB is engaged in illicit practices, using high rates to mask illegal fees or charges.

9. History of regulatory violations:

Research the MSB's history with FinCEN or other financial regulatory bodies. A track record of fines, violations, or sanctions is a clear sign that the MSB has had past issues with compliance.

How to Choose a Compliant MSB as a Customer

When selecting a Money Service Business, it's crucial to screen prospective institutions, and ensure they operate within the bounds of financial laws and have a strong commitment to preventing fraud. Here are some steps you can take:

- **Check for registration with FinCEN:** All legitimate MSBs are required to register with the Financial Crimes Enforcement Network (FinCEN). You can search the FinCEN database to confirm that the MSB is registered and in good standing.
- **Ask about their KYC and AML protocols:** Inquire about the measures the MSB takes to verify the identities of its clients and report suspicious activity. A compliant MSB will be transparent about these policies and eager to demonstrate their commitment to preventing fraud.
- **Verify state licenses and certifications:** In addition to FinCEN registration, MSBs may also be required to obtain state-level licenses. Make sure the MSB you choose is licensed in the state where it operates and adheres to all relevant regulations.
- **Read reviews and reputation:** Look into the MSB's reputation by checking reviews and talking to other businesses that have used their services. A company with positive feedback and a clean compliance history is less likely to engage in or be complicit in fraud.



Case Spotlight: HSI and IRS

<https://www.justice.gov/usao-ut/pr/24-defendants-including-utah-business-owner-accused-running-drug-and-money-laundering>

Georgina Espinoza-Grajeda, 40, of Eagle Mountain, Utah, who is the owner and operator of Multiservicios Lokos LLC, located in South Salt Lake City, Utah, along with her employee Jesid Dadiana De Sutter, 50, of Sandy, Utah, were at the center of a complex conspiracy to secretly and illegally wire millions of dollars in proceeds of narcotics trafficking to suppliers in Mexico and Honduras. Espinoza and De Sutter laundered the money by falsifying wire transfer information to avoid detection. Multiservicios Lokos LLC was allegedly the laundering hub for multiple drug trafficking organizations. Court documents allege that from at least January 2022 to November 2023, Espinoza-Grajeda and De Sutter operated their money remitting business and laundered millions of dollars in drug proceeds deposited by their co-defendants trafficking in fentanyl, heroin, and cocaine throughout the Wasatch Front. Through a collaborative law enforcement effort, agents and officers seized 62,000 fentanyl pills, 24.5 pounds of heroin, 8.5 pounds of cocaine, five firearms, and \$237,000 in cash. Agents and officers estimate the criminal organization laundered more than \$20 million since January 2022.

Did you know?

Since 2018, IRS Criminal Investigation (Cincinnati Field Office), have maintained a Third Party Money Laundering (3PML) Project. This project focuses on Complicit Money Service Businesses (MSB) working for Mexican Drug Trafficking Organizations. The purpose of this project is to develop high-impact 3PML cases for IRS-CI and other agencies across the United States, by utilizing data analytics. This project is known as the "3PML Fentanyl Initiative" (NOTE: Complicit MSB cases involve poly-substance narcotics trafficking and almost always Fentanyl. Additionally, focusing on Complicit MSB's is the clearest avenue for financial investigators to combat the Fentanyl crisis – hence the name "3PML Fentanyl Initiative".)

HSI encourages the public to report suspected suspicious activity through its toll-free Tip Line at [877-4-HSI-TIP](tel:877-4-HSI-TIP). Callers may remain anonymous.

We'd love to hear your thoughts! Please share your feedback to cornerstone@hsi.dhs.gov.



**Homeland
Security
Investigations**

HSI is the principal investigative arm of the Department of Homeland Security (DHS), responsible for investigating transnational crime and threats, specifically those criminal organizations that exploit the global infrastructure through which international trade, travel and finance move.

You are subscribed to receive updates from Homeland Security Investigations (HSI).

[Manage Subscriptions](#) | [Privacy Policy](#) | [Help](#)

Connect with HSI:

[Twitter](#) | [LinkedIn](#) | [Flickr](#) | [YouTube](#) | [HSL.gov](#)

Powered by



[Privacy Policy](#) | [Cookie Statement](#) | [Help](#)

[REDACTED]

From: [REDACTED]
Sent: Friday, August 4, 2023 3:39 PM
To: [REDACTED]
Subject: [EXTERNAL]Working with FinCEN on Geographic Targeting Order on SWB

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

3,250,139 CTRs by all FIs in all of CA in 2024

135,467 of those by MSBs

22,381 where transaction location is in San Diego County

1,528 where transaction location is in Imperial County

2,194,452 CTRs by all FIs in all of TX in 2024

119,098 of those by MSBs

512,430 CTRs by all FIs in all of AZ in 2024

14,195 of those by MSBs

13 in Cochise

765 in Pima

160 Santa Cruz

244 Yuma

43,350 CTRs by all FIs in all of NM in 2024

1,861 of those by MSBs

st_cd	cty_nm	short_zip	count
6 CA	SAN DIEGO	92154	3894
19 CA	SAN DIEGO	92126	2124
35 TX	EL PASO	79903	1467
39 CA	SAN DIEGO	92173	1405
46 TX	EL PASO	79905	1286
63 CA	SAN DIEGO	92101	1072
84 TX	EL PASO	79935	828
86 CA	SAN DIEGO	92117	786
92 CA	SAN DIEGO	91910	730
96 CA	IMPERIAL	92231	689
144 CA	SAN DIEGO	92025	427
146 CA	SAN DIEGO	92113	403
150 TX	WEBB	78040	379
161 TX	WEBB	78041	329
168 TX	EL PASO	79907	316
186 TX	WEBB	78045	268
187 TX	EL PASO	79912	267
190 TX	EL PASO	79938	262
198 TX	EL PASO	79901	249
205 CA	SAN DIEGO	91911	234
209 TX	EL PASO	79936	228
214 TX	EL PASO	79925	219
227 TX	WEBB	78043	205
237 TX	EL PASO	79902	193
246 CA	SAN DIEGO	92105	172
249 TX	WEBB	78046	168
264 CA	SAN DIEGO	92083	142
269 CA	SAN DIEGO	92028	140
278 CA	SAN DIEGO	92021	133
298 CA	SAN DIEGO	92084	115
299 TX	EL PASO	79915	113
304 TX	EL PASO	79924	110
310 CA	SAN DIEGO	91980	107

311 TX	EL PASO	79927	106
312 CA	SAN DIEGO	91945	106
403 CA	SAN DIEGO	91950	57
411 CA	SAN DIEGO	92115	54
412 CA	SAN DIEGO	91942	54
432 CA	SAN DIEGO	91915	49
453 CA	SAN DIEGO	92054	40
457 CA	SAN DIEGO	92104	40
523 TX	EL PASO	79932	28
530 CA	SAN DIEGO	92111	27
531 TX	EL PASO	79929	27
539 CA	SAN DIEGO	92071	26
553 CA	IMPERIAL	92227	25
583 TX	EL PASO	79928	22
603 CA	SAN DIEGO	92123	19
604 CA	SAN DIEGO	92027	19
611 CA	SAN DIEGO	92108	19
657 CA	SAN DIEGO	92069	15
701 CA	SAN DIEGO	92064	13
722 CA	SAN DIEGO	92020	12
733 CA	SAN DIEGO	92120	11
783 CA	SAN DIEGO	92058	9
839 CA	SAN DIEGO	91977	8
845 CA	SAN DIEGO	92026	8
851 TX	EL PASO	79849	7
854 TX	EL PASO	79838	7
885 CA	SAN DIEGO	92078	7
908 CA	SAN DIEGO	92024	6
928 CA	SAN DIEGO	91932	6
1002 CA	SAN DIEGO	92056	5
1083 CA	SAN DIEGO	92121	3
1088 TX	EL PASO	79904	3
1103 CA	IMPERIAL	92243	3
1160 CA	SAN DIEGO	92057	3

1169 CA	SAN DIEGO	92081	2
1175 CA	SAN DIEGO	91902	2
1207 CA	SAN DIEGO	92103	2
1248 CA	SAN DIEGO	92119	2
1260 CA	SAN DIEGO	92128	2
1329 CA	SAN DIEGO	92109	2
1409 CA	SAN DIEGO	92011	1
1410 CA	SAN DIEGO	92019	1
1411 CA	SAN DIEGO	92029	1
1412 CA	SAN DIEGO	92037	1
1413 CA	SAN DIEGO	92040	1
1414 CA	SAN DIEGO	92116	1
1432 CA	SAN DIEGO	92131	1
1471 CA	IMPERIAL	92249	1

Crossing	Zip Code
CALIFORNIA	
San Ysidro	92173
Cross Border Xpress (terminal near Otay Mesa, to Tijuana Airport)	92173
Otay Mesa	92154
Tecate	91980
Calexico West	92231
Calexico East	92231
Andrade	92283
TEXAS - Coahuila	
Boquillas	79834
Amistad Dam	78840
Del Rio	78840
Eagle Pass I and Eagle Pass II	78852
TEXAS - Chihuahua	
El Paso-PDN	79901
El Paso-Stanton	79901
El Paso-Bridge of the Americas	79905
El Paso Ysleta	79907
Marcelino Serna	79853
Fort Hancock	79839
Presidio	79845
TEXAS - Nuevo Leon	
Laredo-Colombia Solidarity	78045
TEXAS - Tamaulipas	
Laredo-World Trade	78040
Laredo Bridge I	78040
Laredo Juarez-Lincoln	78040
Falcon Dam	78545
Roma	78584
Rio Grande City	78582
Los Ebanos	78565
Anzalduas	78572
Hidalgo	78557
Pharr	78577
Donna	78537
Progreso	78579
Los Indios	78567
Brownsville B&M	78520
Brownsville Gateway	78520
Brownsville-Veterans	78521

Cars/Trucks	Pedestrians	
	15,000,000	53,300,000
None		600,000
	6,600,000	15,000,000
	1,600,000	525,000
	7,000,000	4,500,000
	3,000,000	117,600
	400,000	830,000
None		8,319
	65,000	
	1,240,000	84,000
	2,300,000	673,227
	3,400,000	6,188,000
	1,070,000 None	
	7,400,000	517,961
	20,000	10,700,000
Unclear		
Unclear		
	600,000	85,500
	360,000	12,000
	1,145,000	60,000
	1,400,000	1,200,000
	4,600,000	1,800,000
None		147,000
	700,000	280,300
	700,000	17,000
	33,000	40,000
Unclear		
	4,800,000	675,000
	1,950,000	46,000
	320,000	
	900,000	800,000
	800,000	3,000
	2,400,000	154,000
	1,900,000	2,600,000
	2,192,000	100,000

Year of crossing stats	County
	2019 San Diego
First 7 mos of 2016	San Diego
	2019 San Diego
	2,011 San Diego
	2011 Imperial
	2,011 Imperial
	2,011 Imperial
	2,020 Brewster
	2005 Val Verde
	2011 Val Verde
	2011 Maverick
	2006 El Paso
	2006 El Paso
	2,006 El Paso
	2015 El Paso
	El Paso
	Hudspeth
	2011 Presidio
	2006 Webb
	2005 Webb
	2005 Webb
	2005 Webb
	2005 Starr
	2011 Starr
	2005 Starr
	2005 Hidalgo
	Hidalgo
	2011 Hidalgo
	2005 Hidalgo
	Hidalgo
	2011 Hidalgo
	2011 Cameron
	2005 Cameron
	2005 Cameron
	2005 Cameron

Notes

Minor port compared to others.